

The Popularization of Money

Beyond Mr. Hayek's Denationalization of Money

Dr. Bright, 2024

Table of contents

Preface	3
Part I: Twilight of Monopoly	5
§1 The Twilight of the Mint Prerogative	6
§2 Why Fiat Commands Sanctity	13
§3 Inflation and the Complicity of Power	22
Part II: Ideas and Competition	32
§4 The Theory and Dream of Competing Currencies	33
§5 Good Money and Bad Money Revisited	45
§6 Global Ledger and Verifiable Rules	55
§7 Money and the State in Classical Economics	65
Part III: National Banks and Monetary Authorities	76
§8 The Birth and Functions of Central Banks	77
§9 Monetary Policy Tools and Transmission	87
§10 The Boundary Between Fiscal and Monetary Policy	100
§11 Central Bank Digital Currency and Payment Systems	112
Part IV: Transformation by Protocol	123
§12 Bitcoin and the Battle of Standards	124
§13 Incentive Structures in Tokenomics	135
§14 Public Currency and PCIM	145
§15 Private-Domain Stability and On-Chain Assets	166
§16 Time as an Asset	182
Part V: Enterprise Management and Value Networks	189
§17 Corporate Finance and Multi-Currency Management	190
§18 Supply Chain Finance and Private-Domain Settlement	196
§19 Tokenized Financing and Corporate Governance	202
Part VI: Value Networks for AI	209
§20 Silicon Networks and Participants in the Value Internet	210
§21 On-Chain Wallets and Micropayments for Agents	225
§22 The Machine-Readable Value Layer	234
§23 Robots, Compute Markets, and Autonomous Economies	242
Part VII: The Popularization of Money	251
§24 Protocol Collaboration and State Monopoly	252
§25 Paths of Transition	266
§26 The Long-Term Vision of the Value Internet	274
§27 Bad Money Exits: Popular Minting and Free Choice	285
§28 The Endgame of Money	292
Bibliography	298
Glossary	319
Bit gold	331
Epilogue	333

Preface

Preface: Measure, Trust, and the Next Civilizational Chapter

To the Reader

What is the best possible form of a human monetary system? That is an enormous question—and with it in mind, we begin this exploration of monetary theory.

On a weekday in the small hours, a cloud provider bills by the second; the payer is a set of continuously running programs, not a finance director. At the same moment, someone scans to pay fiat at a supermarket, while cross-border remittances still pass through chains of correspondent banks. Two rhythms, two infrastructures, on the same planet—yet rarely discussed in the same book. Humans use money to measure the world, but seldom ask where the measure itself comes from: who may define "how much," who bears the risk of dilution and default, and who can settle with one another without trusting a center.

The subtitle of this book is *A New Chapter in Monetary Civilization: Tribal Tokens • State Fiat • Popular Protocol • Value in Direct Flow*. Four arcs summarize the civilizational history of monetary coordination: from tribal tokens to state fiat, through popular protocol, to value flowing without a single monetary intermediary. If "popularization" is misread as "everyone prints without constraint" or "fiat abolished overnight," it must be clarified first: we abolish the state monopoly of the mint prerogative, not exchange and settlement itself. "Value in direct flow" must be read institutionally—not as a return to barter, but as the possible gradual retreat of state-monopoly money as the sole measure; what is to be eroded by protocolized, verifiable, multi-issuer competitive issuance is not the medium of exchange as such, but the state monopoly of the mint prerogative—the institutional power of a sovereign or legally exclusive issuer to define the unit of account and extract revenue through dilution or implicit levy; competitive minting participation (e.g. PCIM) may still exist, but no longer under a single national exclusive monopoly. The book's central claim, in one sentence: money will not be abolished; the state monopoly of the mint prerogative will—when the bookkeeping, transfer, and issuance rules of value can be publicly verified at low cost, the discipline against abuse shifts from "issuer reputation" to "protocol-verifiable rules." In intellectual lineage, this book takes Hayek's *The Denationalization of Money* as a mirror; it may be read as a step beyond his "denationalization" program: Hayek in the 1970s sought to change who issues¹; this book seeks to change what discipline rests on. State money, central banks, and legal order will persist for the foreseeable future; the question is whether the demand for competing currencies can find a runnable protocol carrier and coexist with state money over the long term.

By "the popularization of money," this book does not urge everyone to print cash. It means that the creation and choice of value measures need no longer be monopolized behind a few gates. Protocols can standardize issuance rules so that collateral, minting, and redemption are auditable and composable—shifting the lens from "mint prerogative" to "protocol prerogative." PCIM (Public Currency Issuance Mechanism) is the abstract issuance framework used throughout; the VRC-10 / Bitgold provisions in the Openverse white paper may be read as one engineering instance of that framework, not as a settled conclusion. The value internet is the long-run name for this transition: open standards aim to do for value transfer what the information internet did for cost reduction and routing.

Artificial intelligence and autonomous agents do not sleep and hold no passports, yet they may need to pay for compute, buy data, and contract on-chain. When payers are no longer only biological individuals, monetary infrastructure grounded in identity and jurisdiction feels cramped—machine-readable value layers and

programmable settlement therefore align with the standardization direction of on-chain protocols. The costs of state-monopoly issuance have never vanished: inflation tax, financial repression, friction in cross-border clearing—these are incentive problems endogenous to monopoly structure. Hayek called in the 1970s for "the denationalization of money"², when globally verifiable issuance rules and low-cost competitive infrastructure were lacking. Today, protocolized ledgers and verifiable scarcity open a new design space: competition and collaboration under open rules, not disorderly over-issuance.

This book uses Hayek's *The Denationalization of Money* as a mirror. We ask how monetary order may evolve in the age of blockchains and open protocols; how corporate management and supply-chain finance may plug into multi-currency ledgers; how autonomous programs may gain machine-readable payment and contracting on a value layer; and how these threads converge toward a vision of the value internet. The appendix includes Nick Szabo's original "bit gold" essay; we avoid investment advice and empty slogans, and technical claims aim to be checkable. These judgments must keep facing tests in cross-border clearing, supply-chain private settlement, and machine-agent payment; if open protocols systematically fail under liquidity crises, governance capture, or regulatory squeeze, the central thesis must be revised accordingly.

注释与引用

1. Hayek (1976), *The Denationalization of Money*, p. 23: competitive schemes aim to make issuers of bad money "at once lead to the rapid displacement of the offending currency by others"—changing who issues and who the market displaces. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
2. Hayek (1976), *The Denationalization of Money*, revised preface (1978), p. 83: monetary schemes would "probably be practicable only as part of a much more far-reaching change in our political institutions"—the technology of the time was insufficient; competition remained on paper. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩

Part I: Twilight of Monopoly

§ 1 The Twilight of the Mint Prerogative

Chapter in brief: The mint prerogative is the right to create and compel circulation of a means of payment—this book argues that when issuance rules can be publicly verified, the center of gravity against abuse may shift from institutional reputation to protocol discipline; money does not disappear; what is eroded is the state monopoly of the mint prerogative, not all competitive minting participation. PCIM is the abstract name for a post-textbook public issuance mechanism; Openverse is one instance of it.

The mint prerogative—who may define, create, and compel circulation of a means of payment—seems a technical and administrative detail, yet it shapes the underlying structure of the entire economic order. This chapter begins from several historical turns and asks: when money is no longer commodity-anchored, when issuers need not redeem holders, how did monopoly harden step by step, and why does it face new questioning today? From Roman silver mines to Nixon's Oval Office, from Frankfurt's printing presses to the genesis block on the internet, every migration of the mint prerogative redraws the boundary between wealth and power. This chapter skips minting craft and focuses on how incentive structures and institutional design change with technology—how power controls the economic order by controlling "the measure of value," and why that control faces, for the first time, a technical interrogation that can be publicly verified. Along this line, the tension between the mint prerogative and popular participation is the starting point of this book's inquiry.

Section 1 The Lesson of Roman Silver Coin

In AD 211, Emperor Caracalla reduced the silver content of the denarius from about ninety percent to fifty. The decision underwent no public consultation, no legislative process, and no announcement to holders—there was no "monetary policy statement" in those days. Merchants were not alarmed at first: the coins still bore the emperor's portrait, still paid taxes, still satisfied courts as legal tender for debts. Money's three functions—unit of account, medium of exchange, store of value—seemed intact in name.

Yet debasement was covert issuance. Halving silver content meant twice as many coins from the same metal; purchasing power shifted from holders to the issuer. Over decades, imperial prices rose and soldiers' real pay was cut in half. During the Crisis of the Third Century (AD 235–284), emperors changed in rapid succession; each successor had to buy army loyalty, loyalty cost fiscal outlays, outlays came from more issuance, more issuance drove inflation, inflation eroded pay, insufficient pay triggered mutiny—a self-reinforcing spiral.

In AD 301, Emperor Diocletian issued the Edict on Maximum Prices, trying to suppress prices by decree, fixing maximum prices for hundreds of goods and kinds of labor, with death for violators. The result was predictable: goods vanished from open markets into black markets; merchants preferred not to trade rather than sell below cost. Goods disappeared, but prices were not truly suppressed, because the root of monetary expansion was untouched. This is among the earliest and best-known price-control failures in history; it shows clearly that trying to suppress symptoms of monetary expansion by command, without changing the incentives for expansion, must have limited effect.

In this history the mint prerogative reveals its true face: not only a public service "guaranteeing fineness," but a tool to dilute wealth. Caracalla financed military spending by lowering silver content; gains flowed immediately into imperial finance, costs were spread across all holders and delayed—by the time prices rose sharply, the political ledger had turned. Hayek, tracing the origins of mint monopoly, noted that this privilege "from the beginning was neither claimed nor conceded on the ground that it was for the general good but simply as an essential element of governmental power"¹—Caracalla's debasement is a classic instance of that logic. This

intergenerational mismatch is mint monopoly's most hidden trait: beneficiaries lock in gains in the present; losers' losses are dispersed over time, hard to attribute, hard to hold to account. Rome's silver mines have been exhausted for two millennia, but this incentive logic never vanished—it only took more modern technical forms.

Section 2 Medieval Monetary Fragmentation: The Cost of Competition and the Lure of Unification

After Rome's collapse, Europe entered a long age of monetary fragmentation. The Carolingians briefly unified coinage, but as feudalism fragmented, local lords, cathedral chapters, commercial republics, even large monasteries minted their own coins of uneven fineness; exchange rates changed every few dozen kilometers. Medieval merchants carried, besides an abacus, often a touchstone and scales to test silver purity—they could trust no issuer's word and had to verify each coin themselves.

Fragmentation imposed huge transaction costs. Historians estimate medieval European inter-city currency conversion fees at five to ten percent of the transaction; moneychangers became indispensable intermediaries, taking substantial spreads on every cross-border trade. Merchants had to master a dozen or more currencies, with rates shifting as mints debased—long-term credit contracts were hard to stabilize: 1,000 livres lent today might mean anything at maturity depending on future coin value, perhaps quietly diluted by a lord needing war funds.

Yet competition also produced positive incentives. The Hanseatic League spontaneously formed monetary agreements across Baltic trade: Lübeck silver, consistently fine, gained credit beyond its issuing region and became a *de facto* standard in northern trade. Venice's ducat served as international currency in the Mediterranean for two centuries—the Republic had no cross-border coercion, but its gold content was repeatedly verified until reputation accumulated to the point that re-assay was unnecessary, and it won. Florence's florin was similar: the Medici built branches across Europe; their bills and coins circulated partly on consistently stable coin quality. This is a real, if limited, local, and costly case of reputation competition producing stability without a central bank, legal tender, or deposit insurance.

Sovereign guarantee of weight and fineness was once genuinely progressive—lowering transaction costs and expanding markets. In fifteenth- and sixteenth-century nation-building, monetary unification and market integration reinforced each other: unified taxation needed a unified unit of account; unified markets needed credible clearing; royal expansion widened the scope of monetary promise. The problem is not unification itself, but the lack of exit after unification, and the end of external competitive constraint once monopoly forms. Stability and monopoly bind unusually tightly in money, hard to separate.

Section 3 From Metal Backing to Central Banking: Constructing Modern Monopoly

As nation-states took shape in the seventeenth and eighteenth centuries, the mint prerogative entered the core of sovereignty, paired with the birth of central banking in the modern sense. The Bank of England was founded in 1694 with a concrete aim: finance William III's war against France. The government borrowed £1.2 million from the Bank, which received the right to issue banknotes in equal amount—war finance and money issuance were bundled from the start, not accidental coincidence.

This pattern replicated across Europe over two centuries: Banque de France (1800, Napoleonic wars), Prussian Bank (1765), Austrian National Bank (1816, post-Napoleonic fiscal reconstruction). Nearly every central bank's founding sat in war finance or fiscal crisis cleanup. Issuance moved from scattered goldsmiths and note issuers to state-chartered institutions, then to exclusive central banks—a process named "monetary modernization" while fusing fiscal and monetary power.

Britain's nineteenth-century gold standard was an important external constraint on expansion: note issue anchored to gold reserves; holders could redeem at a fixed ratio. The Bank Charter Act of 1844 required Bank of England note issue to be backed by gold, constraining issuance from "government will" to "deliverable commodity reserve." In theory the constraint was credible—anyone could exchange pounds for gold; arbitrage made the promise self-enforcing.

Yet the gold standard broke in both world wars—war finance made gold constraints untenable. Britain suspended gold in 1914, restored in 1925 at a wrong rate, abandoned again in 1931; the U.S. banned private gold holding domestically in 1933; Bretton Woods in 1944 established a dollar-centered gold-exchange standard, with the U.S. promising other central banks gold at \$35 per ounce. That was the last formal commodity anchor in international monetary history—and it held only while the U.S. was willing and able to honor redemption.

Central banking is modern concentrated minting: a few institutions set base money; commercial banks multiply on reserves; deposit money the public touches ultimately traces to the apex of this pyramid. Monopoly no longer appears as one king's mint, but as the fiat system's exclusion of substitutes and control of issuance channels—unauthorized issuance faces legal barriers and a credit void.

Section 4 1971: The Last Anchor Disappears

On Sunday, August 15, 1971, President Nixon announced that the dollar would no longer be redeemed for gold at a fixed rate, imposed a ten percent surcharge on imports, and froze wages and prices for ninety days. Bretton Woods formally ended. The surface reason was balance-of-payments pressure and gold outflow—Vietnam war spending, Great Society programs, European central banks redeeming dollars for gold; U.S. gold reserves fell from about \$20 billion in 1958 to about \$10 billion in 1971 while dollar liabilities abroad were several times larger.

Substantively, sovereign states no longer wanted money supply constrained by a commodity anchor. Paul Volcker, Nixon's economic adviser, later recalled the suspension was "temporary," but no serious plan to restore emerged—no international conference mapped a return to gold. Floating exchange rates replaced fixed rates as pragmatic exit, not deliberate redesign. The "Nixon shock" names its suddenness—for the global monetary system, rules changed abruptly, not gradually.

For half a century since, major central bank balance sheets expanded repeatedly. The 1980s–2000s were relatively stable—the "Great Moderation," smooth cycles and stable prices. After 2008, quantitative easing became routine; "unconventional" quickly became "new normal"; after COVID-19 in 2020, Fed assets rose from about \$4 trillion to nearly \$9 trillion in under two years; the ECB and Bank of Japan followed similar paths; the BoJ at one point held more than half of outstanding Japanese government bonds. Money no longer promised redemption in any commodity; the core promise became: this currency pays taxes to government and fulfills domestic contracts—value from institutional compulsion to accept, not deliverable goods.

Consequences appeared on every level. Long-run purchasing power tangled with political cycles and fiscal impulse; ordinary people struggle to separate how much "price rise" is real scarcity versus marginal monetary expansion. Deeper still, after losing an external anchor, constraints on the mint prerogative are only institutional convention and political will—both negotiable and adjustable. Gold supply cannot be legislated upward; code can be changed (with social cost); policy goals reinterpreted; independence eroded—history offers ample examples.

Section 5 Weimar, Argentina, and the Structural Logic of Monetary Collapse

Historical hyperinflations are rarely accidental policy errors; more often they are regular outputs of structure under extreme pressure. Weimar Germany in 1923 is the textbook case. Defeat in World War I, astronomical

reparations under Versailles (ultimately about \$33 billion in gold), French occupation of the Ruhr, left the government facing huge external payments, subsidies for striking workers, and collapsing tax revenue.

Without adequate tax base or international credit, the government printed to fill gaps. Inflation reached triple-digit monthly rates in early 1923; by November, one dollar bought four trillion marks. Workers rushed from work with wheelbarrows of wages to shops; by the next morning the same notes might not be worth transporting. Bakery prices updated hourly; restaurant menus arrived already stale. Hyper-devaluation destroyed money's function as store of value across time; the economy reverted to barter or foreign currency and commodities (butter, coal).

Social consequences ran deep. Middle-class mark savings, life insurance, government bonds vanished; those with foreign income, real assets, or mark debt quickly converted into goods gained wealth. Savers lost to borrowers; fixed income lost to real assets—a redistribution that bred resentment and shaped Germany's political path.

Argentina shows a chronic version: repeated inflation–reform–re-inflation cycles rather than one acute collapse. Argentina underwent at least three large monetary restructurings (1975, 1989, 2001–2002), each ending in exchange collapse or default, with relatively stable intervals between. In 2001–2002 the government froze bank deposits (the *corralito*), forced dollar deposits into pesos, then devalued sharply—depositors lost more than two-thirds in real terms. This is the visible version of mint prerogative abuse: government redefines money by administrative command, transfers wealth, and legal "legitimacy" blocks judicial correction.

The common structure: when government uses the mint prerogative to fill fiscal gaps without effective political or legal constraint, holder interests are eventually sacrificed. Hayek put it plainly: "history is largely inflation engineered by government"². Blame less individual character, more incentive structure.

Section 6 The Symbiosis of Monopoly and Fiscal Policy: Anatomy of Institutional Logic

Monopoly minting and fiscal expansion stand in stable symbiosis—in democracies and autocracies alike, narratives differ, mechanisms resemble. To see symbiosis, dissect incentives, not only outcomes.

Fiscal pressure comes from war, infrastructure, social security, maintaining political coalitions. Open taxation needs legislation and provokes resistance; debt pays interest and must be repaid; debasing money can transfer purchasing power at lower political cost—the "inflation tax" needs no vote; attribution is fuzzy; losers rarely organize effective resistance.

Richard Cantillon's early analysis (c. 1730) of "those nearest issuance benefit first" creates systematic political-economic interests: financial institutions as direct beneficiaries of expansion align with policymakers who favor monetary elasticity. Not necessarily corruption—more often frames like "financial stability" and "job growth"—worthy goals that, when endlessly invoked to justify expansion, hide distributional meaning.

Quantitative easing offers the clearest contemporary distributional illustration (Cantillon mechanism and data in Chapter 3, Section 2)³: order of benefit from new money, gap between asset prices and wage growth, concentrated equity holdings—whatever the causality debate, distributional consequences are built into tools of monopoly issuance.

Section 7 The Commercial Banking System: Covert Extension of the Mint Prerogative

Modern minting is not only central banks; commercial banks participate in money creation. Under fractional reserves, banks are not mere intermediaries recycling deposits—lending creates new money: a loan books as asset (loan) and liability (deposit), and that deposit spends like any other. The Bank of England's 2014 quarterly

Money Creation in the Modern Economy acknowledged this, breaking the textbook "banks intermediate savings" story⁴. Friedman and Schwartz's *A Monetary History of the United States* showed Great Depression monetary contraction amplified through this credit channel into real recession—how banks create money is the hinge extending modern minting through the credit system.

Implications: money creation is dispersed across banks, tied to credit demand, not only central bank injection. In booms, credit demand accelerates issuance, liquidity lifts asset prices, encouraging more borrowing—procyclicality is embedded. In contractions, banks tighten credit, money supply shrinks, deepening demand fall—the main mechanism of Depression-era contraction and the backdrop for lender-of-last-resort and deposit insurance.

For mint prerogative discussion, commercial creation shows monopoly is not only at the central bank but across the government-licensed credit system. Mises in *The Theory of Money and Credit* distinguished "commodity credit" from "circulation credit": the latter expands credit on demand claims without corresponding economic sacrifice—deposit money under fractional reserves institutionalizes this⁵. Entry requires a license, granted by the state, bringing deposit insurance and implicit lender-of-last-resort backstop—a concentrated channel of credit creation, while public chains offer a parallel track to issue tokens without government license; actual payment weight and regulatory boundaries are discussed in Section 8's observables.

Section 8 What Twilight Means

Calling the mint prerogative at "twilight" means its unchallenged monopoly faces more systematic external questioning—not a prophecy that state money vanishes tomorrow. Strictly separate technical possibility (ledgers copyable, rules codable, issuance auditable) from institutional reality (legal tender, clearing permission, regulatory access still concentrated). Infrastructure is necessary, not sufficient; jumping from "tokens can be issued on-chain" to "monopoly has loosened" is an argument leap this section warns against—hence observables and falsifiers, not technical momentum alone.

Outside the usual timeline, monetary technology itself evolves: commodity money to coined metal, metal to redeemable notes, notes to pure credit—each step upgraded record and verification, redefining who may issue, who may verify, who bears risk. Digital technology—first authorized clearing (SWIFT, RTGS), then decentralized public ledgers—continues that arc but poses a new question at verification: can rules of value transfer be independently checked without a single authorized institution? That is twilight's technical context; it still does not mean state money has left center stage.

Some systems have run continuously for years. Bitcoin's mainnet has not seen long interruption since 2009; on-chain nominal transfer volume was on the order of \$19 trillion in 2024; Ethereum contract calls ran in the millions daily in 2023–2024⁶. For stablecoins, Artemis Analytics reported about \$33 trillion global on-chain nominal volume in 2024, mostly exchange internal transfers, market-making loops, and high-frequency bots; Visa Onchain Analytics' "adjusted" twelve-month rolling volume was about \$10.2 trillion after stripping noise; McKinsey and Artemis estimated annual payment volume for goods, services, B2B, and remittances at about \$390 billion—roughly 0.02% of global payments⁷. Three figures coexist: the same on-chain data supports different narratives—using nominal transfer to prove "monopoly broken" is methodologically wrong; using adjusted payments to deny all technical meaning is equally wrong. Verifiable facts: parallel rails exist and scale, but economic weight remains far below fiat.

Sovereign currency competition never stopped, but among states, not Hayek's private rules—which require not only "non-state issuance" but distinguishable units with as stable purchasing power as possible and

adjustable parities after abolishing forced tender. The dollar's share of global reserves fell from about seventy percent in the early 2000s to roughly sixty percent recently per IMF⁸; euro and renminbi rose slowly—geopolitics and macro cycles, not automatic protocol replacement. Some countries dollarize or join the euro; more pursue central bank digital currency (CBDC)—official response to "technology changing payments," upgrading ledger efficiency while keeping monopoly issuance, not abandoning mint prerogative. BIS 2023 surveyed 86 central banks: 93% exploring CBDC, about a quarter in pilot⁹. Bindseil (2024) at the ECB frames retail CBDC as payment-type: non-interest-bearing, holding limits, two-tier operation—avoiding a store-of-value role competing with government debt, not opening Hayekian private competition⁹.

Individuals holding crypto addresses grew from hundreds of thousands to hundreds of millions over a decade; high-inflation economies show more informal dollar and stablecoin use—these show substitutes can gain local legitimacy under some conditions. Record counter-evidence too: in major advanced economies most wages, rent, and taxes still settle in domestic currency; many jurisdictions tighten regulation of unlicensed token issuance, custody, and payment rails; large stablecoin and exchange events since 2022 show on-chain rules can fail through governance, opaque reserves, or legal reach. Substitutes at the margin do not yet mean normative monopoly has dissolved—more like observable exits at the edge, varying by country.

In sum, "twilight" tightens to: mint monopoly will remain dominant for the foreseeable future, but no longer enjoys tacit "irreplaceable, unquestionable" status; how competition unfolds—in what form, jurisdictions, compliance boundaries—must be answered with observables, not technical momentum.

Critics cite on-chain nominal volume, token variety, DeFi TVL to prove "monopoly loosened." That argument must be weighed against adjusted on-chain payment share, fiat share in tax and wages (Section 8⁷)—most advanced economies do not support "end of monopoly." Ma et al. (2023) and Chainalysis geographic reports suggest marginal-corridor adoption reflects exit options when fiat anchors fail¹⁰, not institutional turning points from single-chain TVL. The more defensible claim is verifiable constraint carriers, not ended monopoly.

From Roman debasement to Weimar hyperinflation to post-2008 balance sheet expansion and Bitcoin's genesis block—monetary history records who holds the measure of value and who pays the cost. Quality of competition depends on information symmetry, enforceable rules, and ease of entry and exit; how fiat belief is sustained and inflation incentives work must be read in this coordinate system.

注释与引用

1. Hayek (1976), *The Denationalization of Money*, p. 28: "From the beginning the prerogative was neither claimed nor conceded on the ground that it was for the general good but simply as an essential element of governmental power." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
2. Hayek (1976), *The Denationalization of Money*, p. 33: "history is largely inflation engineered by government." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
3. Systematic analysis of QE, Cantillon effects, and asset-wage gaps in Chapter 3, Section 2; equity concentration per Federal Reserve Survey of Consumer Finances. ↩
4. McLeay, Radia & Thomas (2014), "Money Creation in the Modern Economy," *Bank of England Quarterly Bulletin* 2014 Q1, pp. 14–27. <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy> ; Friedman & Schwartz (1963), *A Monetary History of the United States*, ch. 7. ↩
5. Mises (1912), *The Theory of Money and Credit*, Liberty Fund 1980 ed., pp. 264–266: circulation credit expands without the creditor's corresponding economic sacrifice. <https://www.econlib.org/library/Mises/msT.html> ↩

6. Bitcoin 2024 on-chain nominal transfer ~\$19T (Riot Platforms VP Pierre Rochard, Cointelegraph 2025-01-04); cumulative nominal Glassnode ~\$131T with entity-adjusted far lower. Ethereum contract call frequency is public-node/browser magnitude, varies by metric. ↩
7. Artemis Analytics ~\$33T global stablecoin on-chain nominal volume 2024; Visa Onchain Analytics Dashboard (2025) adjusted 12-month ~\$10.2T; McKinsey & Artemis, *Stablecoins in payments: What the raw transaction numbers miss* (2025) ~\$390B/year real payments ~0.02% global; Lyons & Viswanath-Natraj (2020), NBER WP 27136; Coin Metrics (2024), *State of Stablecoins*. ↩ ↩²
8. Dollar share of allocated global reserves: IMF COFER ~71% around 2000, ~58% Q4 2024 (quarterly variation)—competition remains among state monies, not private protocol share. ↩
9. BIS (2023), *BIS Papers* No. 125; Boar, Holden & Wadsworth (2021), *BIS Papers* No. 114; Bindseil (2024), ECB Occasional Paper 322. <https://www.bis.org/publ/bppdf/bispap125.htm> ; <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op322~5822218919.en.pdf> ↩ ↩²
10. Bullmann, Klemm & Pinna (2019), ECB Occasional Paper 230; Gadzinski et al. (2024), *International Review of Financial Analysis* 96, 103608; Ortiz & Witte (2023), BIS WP 1137; CFTC Staff Report (2022); Ma et al. (2023), IMF WP 23/72. ↩

§ 2 Why Fiat Commands Sanctity

Chapter 1 traced how the monopoly of the mint prerogative hardened through history; this chapter asks where the everyday beliefs that sustain that monopoly come from.

In Chinese, *fabi* (“fiat money”) carries an almost natural aura of authority: once the law names it, paper seems to acquire a soul. Yet what, precisely, does the law confer—value inherent in the money itself, or an obligation to use it? Between these two lies a subtle but decisive fissure. What the law confers is *legal tender* status: under specified conditions, refusal to accept that money carries legal consequences. The law does not endow the money with intrinsic value, nor does it guarantee purchasing power. Once this distinction is clear, the “sanctity” of fiat shifts from metaphysical authority to a social institution that must be continually maintained. This chapter examines, section by section, the sources of fiat’s standing; the psychological and institutional mechanisms that sustain its daily operation; how sanctity peels away under extreme pressure; and what the identity of “the sole lawful money” means today, when plural units of account are becoming technically feasible.

Section 1. Tax and Contract: Two Institutional Chains

The foundation of fiat status lies in the tax obligation. When government requires taxes to be paid in the domestic currency, economic agents must hold that currency in their receipts and payments, whether or not its purchasing power is stable. Hayek, discussing legal-tender status, observed that “legal tender” in the strict sense means only a means of discharge that a creditor may not refuse; it does not confer intrinsic value on the money. What truly sustains the circulation of fiat is often the institutional chain formed by taxation and the performance of contracts¹. This mechanism is treated by Modern Monetary Theory (MMT) scholars (such as L. Randall Wray and Stephanie Kelton) as the core of money’s “stateness”—a lineage that can be traced to Knut Wicksell and Abba Lerner’s “functional finance”: the state spends first and creates money, then recovers it through taxation, thereby maintaining the circulatory loop. Whether one accepts or rejects this theoretical frame does not affect the factual basis it describes: so long as the tax obligation exists, demand for the domestic currency will not fall to zero, because the only lawful means of discharging tax obligations is that currency.

Historical practice makes the logic vivid. A common device of colonial governments after conquering new territories was to require local populations to pay a hut tax in the metropolitan currency, thereby forcibly creating demand for that currency—residents had to enter the money economy to obtain it, and thus supply labor and join the colonial economy. In the colonial history of Africa, the expansion of sterling and franc circulation zones often moved in step with the introduction of compulsory tax obligations. Outcomes were not settled by the market; institutional compulsion was the driver².

The tax anchor has a still older theoretical formulation: Chartalism, beginning from Georg Friedrich Knapp’s *The State Theory of Money* (1905), holds that the monetary unit is first defined by the sovereign through systems of account and clearing, while taxation is the closed-loop link that recovers money in circulation and sustains its value³. MMT’s modern restatement of the “spend first, tax later” cycle stands in the same lineage. Accepting this frame does not automatically entail that “monopoly issuance is forever optimal”—it only shows that under existing tax law, demand for the domestic currency has an institutional floor. A floor is not sanctity: Zimbabwe still required taxes to be paid in the domestic currency’s name during hyperinflation, yet holders raced to convert receipts into dollars or goods. Technical and black-market channels for alternative units of account have repeatedly appeared at the margins; tax and compliance remain bound to the domestic currency and still dominate within the foreseeable institutional core—these must be stated separately and not conflated.

The second chain is debt and judgment: contract denomination and the enforcement of court judgments are ordinarily in fiat; in most jurisdictions, refusal to accept it is not a lawful defense against a creditor. A creditor holding a judgment denominated in the domestic currency can compel discharge in that currency through legal execution, whatever means of payment the debtor prefers. The binding of legal language to fiat places the entire commercial credit system on a single unit-of-account track; any agent that wishes to operate in the formal commercial environment must accept this fact.

Fiat thus becomes the default language of economic activity—not because it is optimal in every setting, but because it is embedded at the deepest layer of legal structure. Alternative means of payment often must still be converted into fiat to satisfy tax and compliance obligations. This nesting produces powerful network effects: the more people use it, the harder it is for any single holder to exit, because every counterparty prices in fiat. Economists call this a “coordination equilibrium”—among multiple possible monetary equilibria, history, law, and custom jointly lock in the present choice, even when theoretically superior alternatives exist. Neither chain is natural: the form of tax obligation is a policy choice, and contractual conventions of denomination can be eroded by market pressure. Fiat sanctity, therefore, is far from an unshakable axiom of nature.

Section 2. The Historical Construction of Sanctity

The “sense of sanctity” surrounding fiat is the product of continuous construction across generations; it did not descend from nowhere. In the nineteenth-century formation of the nation-state, monetary unification was invested with symbolic meaning beyond economic function: one money meant one economic community, and notes bearing the emperor’s or founding father’s likeness were everyday media of national identity. After unification in 1871, the German Empire introduced the mark and consolidated the varied currencies of dozens of prior states into an imperial medium of exchange—this was not only economic convenience but the symbolic completion of national unity: “we use the same money” and “we are one nation” were deeply bound in ideology.

The educational system played a key role in this construction. Economics textbooks teach the functions of money—medium of exchange, unit of account, store of value—against a default fiat background, rarely asking why these three functions must be performed by one and the same money, monopolistically issued by government. Hayek rebutted the naïve belief that “money must be invented and supplied by the state,” noting that this superstition “has been wholly displaced by our understanding of the spontaneous generation of such undesigned institutions by a process of social evolution of which money has since become the prime paradigm (law, language, and morals being the other main instances)”⁴—parallel currencies were historically not rare: border towns used both countries’ coins; colonies circulated metropolitan and local paper; mid-twentieth-century dual-track systems with official and informal market rates coexisted in many countries. “One country, one money” is the output of a specific historical process in the nineteenth and twentieth centuries, not a necessary corollary of economics.

Everyday language further reinforces this standing. “Cash,” “real money,” and “hard currency” often default to fiat; crypto assets were long called “virtual currencies,” implying secondary status; goods are priced in the domestic unit, and wage slips and invoices need no explanation of their unit of account—they exist like air, unnoticed. When media report economic data—prices, wages, GDP growth—every figure takes the domestic currency as the default unit, so that currency’s “centrality” is quietly repeated in every reception and transmission of economic information. Over time, the public confuses fiat with “value itself,” rather than distinguishing it as “a unit of account backed by government.” From the standpoint of institutional designers, this confusion is useful: it lowers the public’s willingness to “vote with their feet” and reduces active challenge to the monetary regime.

Section 3. Multiple Sources of State Credit—and Its Fragility

Beyond the two hard constraints of tax obligation and debt performance, fiat sanctity rests on a softer but equally important dimension: state credit. State credit arises not only from legal compulsion but from public expectations of the state's future taxing capacity, policy stability, and institutional continuity. A country with sound debt management, predictable policy, and stable institutions often obtains a trust premium for its money beyond what legal compulsion alone can explain—holders believe that even if the government does not compel acceptance tomorrow, the money will still be a good store of value. Conversely, in a politically turbulent country with uncontrolled debt and unstable institutions, even complete legal-tender status will see the actual range of acceptance shrink sharply, as holders seek every lawful or informal channel into more stable substitutes.

The monetary meaning of state credit has a powerful theoretical expression: the value of state money equals a partial claim on the state's future taxing capacity. To hold money is, in substance, to hold a broad right of participation in the nation's economic activity—the ultimate source of the goods and services that money can buy is the labor and capital of other economic participants operating under the same legal system. The stronger the state's taxing capacity (depending on economic scale and an effective tax apparatus), the thicker the credit base of the money. This frame explains why small open economies typically cannot issue currencies widely accepted in international markets—their tax base is relatively limited, and the span of state-credit backing is narrow; it also explains why the dollar and the euro attain reserve status—the economies behind them are large enough to support large-scale holders of the currency with credit.

The fragility of state credit is especially salient against a background of chronically accumulating fiscal deficits. When the ratio of government debt to GDP keeps rising, markets begin to question whether future taxes can cover principal and interest; state credit then faces pricing pressure from the bond market—reflected in rising interest rates as a credit-risk premium. This pressure is asymmetric between sovereign-currency issuers and non-sovereign-currency issuers: the former (such as the United States, the United Kingdom, and Japan) can partly evade market pressure through money creation, at the cost of potential inflation risk—how the fiscal-monetary boundary is eroded, and how the inflation tax operates; the latter (such as euro-area member states and dollarized countries) face market punishment directly, without the buffer of monetary policy. This is a structural asymmetry in fiat credit, a systemic institutional disadvantage for non-sovereign issuers—in 2010 Greek government debt to GDP once exceeded 130 percent, and ten-year yields broke 30 percent in 2012, forcing acceptance of troika rescue; over the same period U.S. federal debt to GDP was higher still, yet financing continued in dollars with the buffer of “one's own central bank”⁵. The contrast shows: legal-tender status and the tax anchor can sustain *nominal* circulation, yet they cannot prevent *real* purchasing power and financing conditions from repricing credit.

Section 4. The Boundaries of Legal Compulsion and Historical Exceptions

Fiat's legal status must be understood within concrete legal frameworks, and that understanding is often more complex than the public usually assumes. The meaning of “legal tender” is not identical across countries, nor has it always equated historically to “the sole lawful means of payment.” In the United States, federal law makes the dollar legal tender for all public and private debts, yet private parties may lawfully agree on other means of payment—gold clauses were once common in American contracts until the Roosevelt administration abolished them by executive order and congressional legislation in 1933, citing the need to preserve the effectiveness of national monetary policy. The abolition of gold clauses itself reveals a fact easily overlooked: the “sanctity” of legal-tender status is not immemorial; it was reinforced and maintained through active legal intervention under particular political-economic conditions.

Britain's situation is subtler: Bank of England notes are unlimited legal tender in England and Wales, yet do not have legal-tender status in Scotland (Scotland has locally issued banknotes with a distinctive legal standing); euro-area member states recognize the euro as legal tender, yet merchants retain the right to refuse certain denominations (such as very large notes), and private agreements specifying other means of payment are lawful. Hong Kong's monetary system has three commercial banks issuing Hong Kong dollar notes under the Hong Kong Monetary Authority's oversight; legally the Hong Kong dollar is legal tender, yet behind it stands a currency-board regime strictly pegged to the U.S. dollar—a special form of monetary sovereignty, with its own distinctive arrangement between legal text and economic reality.

These legal details reveal a general pattern: legal tender protects the creditor's right not to be "unreasonably refused," and plays a decisive role mainly when contractual disputes enter judicial procedure; at the level of *ex ante* transactional choice, willing parties retain considerable flexibility—the law does not compel every everyday transaction to be conducted in the domestic currency. In practice, however, that flexibility is constrained by extensive institutional friction: employers pay wages in fiat because labor law usually sets the minimum wage in the domestic unit; landlords collect rent in fiat because mortgage collateral and property taxes are calculated in fiat; tax filings are denominated in the domestic unit and run through all economic activity. Every seemingly "voluntary" use of fiat has, behind it, an institutional chain linking it to some node of legal compulsion. Fiat sanctity is therefore the product of an institutional network as a whole, not the effect of a single statutory clause.

Section 5. Zimbabwe: An Extreme Test of Sanctity

When institutional habit meets the collapse of purchasing power, sanctity fades quickly. Zimbabwe's hyperinflation in the 2000s has been cited countless times, yet its inner mechanism rewards careful reconstruction: it offers not only an extreme case but a mirror reflecting the nature of fiat sanctity.

The Mugabe government launched land reform in 2000, confiscating white-owned farms for distribution to veterans; agricultural output plunged, export earnings collapsed, foreign exchange dried up, while government spending did not contract accordingly. Fiscal deficits were filled by printing, and inflation accelerated. The government's initial response was price controls—goods could not be sold above a stated price. The result echoed Diocletian's Edict on Maximum Prices: store shelves emptied, goods vanished from formal channels, yet remained obtainable on the black market at prices reflecting actual inflation. Economic activity shifted from the observable formal economy into an informal economy hard to measure.

By 2008, hyperinflation entered an exponential phase. Steve Hanke, professor of applied economics at Johns Hopkins University, estimated from official and black-market price series that Zimbabwe's monthly inflation peaked around 79.6 billion percent in November 2008 (about $7.96 \times 10^{10}\%$), implying an annualized Hyperinflation Index on the order of 89.7 sextillion percent—a rare extreme in human monetary history⁶. Legal status remained intact—the Zimbabwean government never declared the domestic currency void—yet economic participants raced to convert receipts into U.S. dollars, South African rand, or physical goods, completing purchases within whatever window price tags could still hold. The money was still "lawful," yet no longer performed as a store of value, and barely as a medium of exchange—merchants priced in dollars; accepting the domestic currency required immediate conversion, and the conversion rate changed by the hour.

In January 2009, the Zimbabwean government formally allowed the dollar, the rand, and other foreign currencies as lawful means of circulation, in effect acknowledging that the domestic money had lost its functional sanctity; that same year the central bank issued a note of 100 trillion Zimbabwean dollars, which on the day of issue could buy goods that within a week had shrunk to a fraction. In legal form, the Zimbabwean dollar was not

formally discontinued until 2015⁶; for those six years it had already been discarded by the market—a legal label could not rescue a unit of account that had lost trust. Extreme cases act as a magnifying glass: fiat’s power comes from its acceptance circle; when that circle contracts, the legal label cannot retrieve it. Zimbabwe lights the boundary of fiat sanctity most brightly: tax obligations can sustain formal demand for the domestic currency, yet cannot alone sustain its sense of sanctity; the latter depends on continuous maintenance of purchasing power and expectations—once they collapse, the institutional chains remain, but everyday belief is gone. Note carefully: Gresham’s law under fixed legal parity (bad money drives out good) and “good money wins” under floating conditions are two directions of displacement under different institutional premises; they must not be conflated as a “Gresham inversion”⁷—Section 2 of Chapter 5 on Thiel’s M-money ranking, and Section 7 of Chapter 7 on the Hayek–Gresham contrast, offer further reading.

Section 6. Dual-Track Prices and the Margin of “Voting with One’s Feet”

Fiat sanctity is fully maintained only within closed borders. Once a comparative benchmark appears, cracks show at once—and that benchmark often emerges where least expected. China’s foreign-exchange certificate (*waihuiquan*) system in the early reform era is a classic case: FEC and renminbi each had their circulation circles; goods obtainable with certificates were superior in quality and supply to channels that accepted only renminbi, creating divergent evaluations of the two monies. Officially they were held equivalent, yet market behavior clearly expressed the difference—FEC traded at a premium on the black market.

The same logic appears in more general form in foreign-currency deposits in high-inflation countries. Argentine residents in successive crises have held large amounts of dollar cash—sometimes even under mattresses at home, the so-called “mattress economy”—rather than saving in the domestic currency. This is less irrational speculation than a transparent price on trust in the monetary regime: the domestic currency for everyday transactions, foreign currency for the store of value. When the two functions are borne by different monies, the domestic currency’s full “moneyness” has partly unraveled, even if it remains legally the sole legal tender.

During the sharp depreciation of the Turkish lira in 2022–2023, households and firms steadily increased foreign-currency and FX-hedged deposits: Turkish central-bank statistics show that residents’ foreign-currency deposits as a share of broad money (M2) once exceeded 50 percent in 2023, with corporate foreign-currency deposits also rising markedly⁸. At the same time, administrative intervention in central-bank personnel and interest-rate policy ran alongside official intervention in the exchange market, and the gap between official and parallel-market rates widened. This is a modern case of tension between “legal sanctity” and “economic reality”: the government continues to insist on the domestic currency’s standing; the market continues to seek exits for transferring value. The spread itself is an observable indicator, yet one must avoid leaping from “rising foreign-currency deposits” straight to “the domestic currency is about to be replaced”—the lira remains the primary unit for wages, rents, and most retail prices; dollarization here appears first as a division of labor in the store-of-value function, not as wholesale replacement of the medium of exchange.

Section 7. Stablecoins and Digital Money: New Challengers to Sanctity

Over the past decade, the expansion of dollar-denominated stablecoins has provided the latest observational sample of fiat substitution—but observation must keep a strict perimeter. Programmable on-chain settlement and 24/7 transfer are already technically feasible; tax, legal tender, and retail still centered on the domestic currency remain the institutional norm: stablecoins already perform settlement functions in specific settings, yet have far from unsettled fiat’s central place in the institutional network. Section 8 of Chapter 1 has systematically

discussed the difference between nominal on-chain volume and adjusted payment volume⁹; Coin Metrics’ 2024 report put the aggregate market capitalization of major stablecoins above \$150 billion; McKinsey and Artemis jointly estimate that real payment flow after stripping exchange recirculation is about \$390 billion per year—an extremely small share of global payment flows. Using nominal on-chain volume to prove that fiat has “already been replaced” is as dangerous as methodological error.

The expansion of dollar stablecoins is largely an extension of dollar credit into on-chain environments at lower friction, rather than a direct “challenge to dollar sanctity”—most reserve-backed stablecoins are backed by dollar assets or equivalents, and regulatory frameworks have evolved around “dollar extension” rather than “sovereign substitution” (Gorton & Zhang 2022 analogize them to a “wildcat banking” form in need of stronger regulation⁹). In this process the dollar has, if anything, expanded its circulation range into markets that traditional U.S. banking cannot directly serve. Genuine rule competition comes from native crypto assets—Bitcoin, Ethereum (ETH), and others that are not pegged to any fiat, with issuance rules fixed in code and not amendable by a single sovereign—yet as of 2024 their price volatility still makes them poor vehicles for everyday pricing; in major advanced economies, wages and invoices are almost never denominated primarily in BTC/ETH.

Central banks’ responses vary: some advance central bank digital currency (CBDC) plans; some tighten regulation to suppress unlicensed stablecoins; some seek balance through observation and strategic play. Whatever the strategy, fiat sanctity faces a new proposition: in a programmable-money environment, what exactly is the advantage of “legal” status, and how does it compete for credibility with rule constraints realized in technology? Ultimately this depends on how institutions define the division of labor between legal tender and programmable rules—private tokens have not yet won a comprehensive contest, but the boundary of that division is being renegotiated.

Section 8. Central Bank Digital Currencies: The State’s Active Defense of Digital Sovereignty

Facing challenges from crypto assets and stablecoins, central banks have widely chosen to develop CBDCs—this should be understood as institutional experiment, not as a proven defense of sanctity. A BIS 2023 survey of 86 central banks found that 93 percent of respondents were exploring CBDCs, with about a quarter already in pilot stages¹⁰; yet the distance between “exploration” and “everyday replacement of private payments” remains large.

China’s digital renminbi (eCNY) has the largest pilot scale: the People’s Bank of China disclosed that by June 2023 cumulative transactions in pilot regions amounted to about RMB 1.8 trillion, with some 120 million personal wallets opened—substantial volume, yet still far smaller than contemporaneous mobile-payment flows (such as Alipay and WeChat Pay)¹⁰. The ECB’s digital euro project, Federal Reserve research white papers, and the BIS-coordinated multilateral mBridge experiment are all institutional responses of national monetary systems to the digital-age challenge; their shared assumption is that if a digital form of fiat can match stablecoins in convenience, programmability, and velocity of circulation, the public will have no reason to turn to privately issued digital money. This is a logic of policy design, not a completed empirical conclusion.

CBDC design seeks to “internalize” some functional advantages of stablecoins into the state monetary system—programmable disbursement (e.g. consumption vouchers), offline payment, fine-grained control, and so on. Yet rollout faces two sharply different obstacles: tensions among interoperability, privacy protection, and regulatory compliance make engineering complexity far exceed public perception; CBDC programmability also makes “money with usage restrictions” a technical reality, sparking debates over surveillance and monetary freedom—the digital euro project has met political pushback in the European Parliament demanding that “cash be preserved and

transaction privacy protected.” Nigeria’s eNaira, with its weak adoption, provides a counter-sample: government can launch a CBDC; the market need not use it daily—network effects and real pain points cannot be solved by administrative deployment alone. The defense of fiat sanctity must not come at the cost of eroding citizens’ confidence in freedom of monetary use; whether CBDCs can deliver incremental value while preserving trust remains to be tested on national mainnets and in the courts.

Section 9. The Functional Boundaries of Sanctity

What most deserves interrogation about fiat sanctity is its functional boundary: where it provides irreplaceable coordination; where compulsion produces net harm; and where technological progress allows the boundary to be redrawn.

This boundary awareness helps judge which domains suit innovation and competition at the protocol layer, and helps explain why certain narratives of “replacing fiat” meet real resistance—fiat does provide hard-to-replace coordinating value in specific functions, and that value is rooted in institutional networks accumulated over generations.

For the foreseeable long run, fiat will still dominate taxation, domestic contract denomination, government transfers, and most retail transactions; that standing depends on the continuous operation of state compulsion and institutional networks, not on a demonstration of competitive advantage. Tax law requires payment in the domestic currency; transfers and retail pricing are deeply embedded in the same network—switching costs and coordination inertia keep the present choice stable for a long time.

Cross-border remittances, programmable contract execution, store of value under high inflation, and financial access for the unbanked constitute settings where sanctity faces substantive challenge: under technical or institutional constraints fiat cannot serve efficiently, and substitutes compete on functional performance rather than ideology. Verifiable on-chain rules and cross-border settlement via stablecoins have already been partially realized at the margins; global flow weights, the tax anchor, and clearing permissions still lean heavily toward fiat—one should not infer the unraveling of the core regime from success at the margins. Sanctity continues within its functional boundary; space beyond that boundary is being rewritten—this is a gradual adjustment of institutional division of labor, not an assertion that state money is about to vanish.

From a more macro institutional perspective, discussion of fiat sanctity ultimately points to the basis of money’s legitimacy: historically two answers have coexisted—sovereign legitimacy (conferred by the state) and market legitimacy (voluntary acceptance by participants). Hayek argued that only by abolishing the government’s monopoly of money issuance and removing compulsory legal-tender status can the public freely choose among currencies by purchasing power—“Good money can come only from self-interest, not from benevolence”¹¹. Pure sovereign legitimacy collapses under extreme inflation; pure market legitimacy, without an external anchor, can generate instability. Their combination—the state providing a stable legal frame, the market providing continuous evaluation of monetary quality—is in practice the most common sustainable form of monetary institution.

Blockchain protocols introduce a third source of legitimacy: algorithmic legitimacy—the transparency and verifiability of rules, enabling strangers to inspect conditions of issuance and transfer without mutual trust. This remains a proposition to be tested on mainnets and at regulatory boundaries; one cannot leap from “code is public” to “trust has already migrated.” The relative weights of the three sources of legitimacy are being reallocated in present institutional evolution; this chapter focuses on how everyday beliefs and institutional chains sustain the sense of sanctity, and where that sense peels away.

Fiat's institutional nesting is also a form of "information compression": countless dispersed credit assessments and risk pricings are simplified into the coordinating outcome of "using the same money." When people use the same money, they can transact without knowing one another's creditworthiness—this is money's core contribution to lowering transaction costs. The verifiable rules of blockchain protocols offer a different path of information compression: legal status unifies the unit of account, while on-chain inspectable rules and state enable strangers to interact without mutual trust. Each path has its applicable scene boundary; to think the popularization of money at the institutional rather than merely technical level, one must first see this difference clearly. Fiat sanctity need not be overthrown, yet it must be precisely located—knowing where it is strong and where it is fragile allows one to lean on it where it is strong, and to seek better substitutes where it is fragile.

注释与引用

1. Hayek (1976), *The Denationalization of Money*, p. 36: "In its strictly legal meaning, 'legal tender' signifies no more than a kind of money a creditor cannot refuse in discharge of a debt due to him in the money issued by government." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
2. Helleiner, Eric (2003), *The Making of National Money: Territorial Currencies in Global History*, Cornell University Press, ch. 2 (colonial hut tax, territorial monetization, and forced circulation); Austin, Gareth, and William Darity Jr. (2007), "The Historical Origins of Inflation Targeting," *Journal of Post Keynesian Economics* 29(4), pp. 635–660 (survey of African colonial hut-tax cases). <https://doi.org/10.2753/PKE0160-3477290408> ↩
3. Knapp, Georg Friedrich (1905/1924), *The State Theory of Money*, English trans. Macmillan, ch. 1 (chartalism, unit of account); Innes, A. Mitchell (1913), "What is Money?" *Banking Law Journal* 30(5), pp. 377–408 (credit theory of money; tax acceptance circle). <https://www.community-exchange.org/docs/Innes/>; Wray, L. Randall (2012), *Modern Money Theory*, Palgrave, ch. 2 (modern restatement of the tax anchor). ↩
4. Hayek (1976), *The Denationalization of Money*, pp. 36–37 (Chapter 5, "The Mystique of Legal Tender"): "This belief has been wholly displaced by our understanding of the spontaneous generation of such undesigned institutions by a process of social evolution of which money has since become the prime paradigm (law, language, and morals being the other main instances)." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
5. Greek government debt to GDP: Eurostat 2010–2012 series; ten-year sovereign yields: Bloomberg / ECB Statistical Data Warehouse, May 2012 peak. U.S. federal debt to GDP: FRED series GFDEGDQ188S. The contrast illustrates the sovereign-currency buffer; it does not argue for U.S. fiscal sustainability. ↩
6. Hanke, S. H. & Krus, N. (2013), "World Hyperinflations," *Cato Working Paper*; Hanke, Zimbabwe Hyperinflation Index updated through November 2008 (monthly inflation peak about 79.6 billion %). Formal discontinuation of the Zimbabwean dollar: RBZ 2015 announcement, old Zimbabwe dollars ceased circulating as of 30 June 2015. <https://www.cato.org/research/working-papers/world-hyperinflations> ↩ ↩²
7. On Thiel's reading, see Section 2 of Chapter 5; on the Hayek–Gresham / Thiel boundary and Rolnick–Weber's "Gresham's fallacy," see Section 7 of Chapter 7. Goodhart (1998) on the M-money / C-money frame: Section 2 of Chapter 5 and Section 1 of Chapter 7. ↩
8. Residents' and firms' foreign-currency deposits as a share of M2: Turkish Central Bank (CBRT), Monetary and Financial Statistics, 2022–2023. Administrative intervention in central-bank personnel and interest rates: see Section 4 of Chapter 3. ↩
9. Coin Metrics (2024), *State of Stablecoins 2024*: stablecoin market capitalization and peg-deviation benchmarks; McKinsey & Artemis, *Stablecoins in payments: What the raw transaction numbers miss* (2025): nominal on-chain volume vs. adjusted payment volume (about \$390 billion/year). Gorton & Zhang (2022), *University of Chicago Law Review* 89(1), pp. 1–52: "wildcat banking" regulatory frame for fiat-reserve stablecoins. On the three-perimeter difference in on-chain flow, see Section 8 of Chapter 1. ↩ ↩²

10. BIS (2023), "CBDCs: Progress and ongoing work," *BIS Papers* No. 125: survey of 86 central banks; People's Bank of China, *Progress of Research & Development of E-CNY in China* (2021) and mid-2023 disclosures of pilot transactions and wallet data. ↩ ↩²
11. Hayek (1976), *The Denationalization of Money*, p. 131: "Good money can come only from self-interest, not from benevolence." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩

§ 3 Inflation and the Complicity of Power

Once the “aura of the sacred” around fiat money loosens, inflation becomes the touchstone of institutional honesty. This chapter follows that thread.

In the macroeconomic accounts inflation is a monetary phenomenon; in kitchens and supermarket aisles it is a lived one. The number printed on a banknote stays the same while the eggs it buys grow fewer—that gap arises from institutional mechanisms, not from accidental miscalculation. Starting from incentive structure, the chapter examines how monopoly issuance facilitates fiscal expansion, who bears the cost, and how this complicity has replayed across political regimes and historical periods. The complicity of inflation and power does not require any particular villain; it is nested in institutional design: any agent that holds a monopoly on money issuance, however benevolent its starting motives, faces incentives tilted toward expansion. Hayek observed that inflation not only erodes purchasing power but also makes “effective capital and cost accounting” impossible¹. Only by seeing this structure clearly can one grasp why external constraint is indispensable—whether that constraint comes from a commodity anchor, legal independence, or protocol-layer rules.

Section 1. The Hidden Tax: Anatomy of the Inflation Tax

Open taxation must pass through legislative procedure, must be bargained among political interests, and remains visible so that voters can assign responsibility. Inflation dilutes the real value of cash and fixed claims; the effect resembles taxation, yet is more dispersed and harder to attribute: no published tax rate, no assessment notice, no tax official to hold to account—only price tags that quietly shift on the shelf.

When government debt is denominated in the domestic unit of account, unexpectedly high inflation reduces the real burden of repayment. Suppose the government borrows 10 billion at a 5 percent nominal rate; if cumulative inflation over a decade cuts purchasing power by 40 percent, the real resources repaid fall well short of those borrowed—creditors’ losses are the government’s implicit write-down. The mechanism is especially sharp when the same government is both the largest debtor and the issuer of the currency. If bondholders are mainly domestic private savers, wealth is transferred from savers to the state; if foreign holders own much of the debt, the effect of domestic inflation on external liabilities also depends on the exchange-rate path, yet the erosion of domestic purchasing power remains.

Keynes gave a precise description of this mechanism in *A Tract on Monetary Reform* (1923), and explicitly labeled it dangerous. He wrote that through monetary expansion governments can confiscate “secretly and unobserved, an important part of the wealth of their citizens,” and warned that prolonged reliance on the device would destroy the public’s trust in the monetary order². The passage is often stripped from context and used as ammunition against Keynesianism; yet when Keynes wrote it he was defending monetary stability, not inflation. His later countercyclical fiscal theory was developed into macroeconomic policies favoring deficit spending—creating a complex tension with his clear critique of the inflation tax here, a tension never fully resolved in Keynesian policy practice.

The special danger of the inflation tax lies in its temporal mismatch and fuzzy attribution. Benefits arrive in the present: the government gains additional purchasing power, and the first recipients of new money can complete transactions before prices respond. Costs are spread into the future: when prices rise, holders of money and fixed claims absorb the loss, but by then a temporal distance has opened between the issuance act and the injury, and the causal chain is no longer intuitive. In *The Theory of Money and Credit*, Mises defined inflation precisely as “an increase in the quantity of money (in the broader sense of the term, so as to include

fiduciary media as well), that is not offset by a corresponding increase in the need for money ... so that a fall in the objective exchange value of money must occur”³—a formulation that restores inflation from vague political rhetoric to a testable quantity proposition. Politically, no “inflation-tax” bill is delivered to the taxpayer; without an accountable taxing act, organized political resistance is hard to mount.

Section 2. The Cantillon Effect: Who Gets the New Money First

“Newly created money does not fall evenly upon the economy”—this observation originates with the eighteenth-century Irish economist Richard Cantillon. In *An Essay on Economic Theory* he described how the effects of monetary expansion depend on the path by which new money enters the economy: agents nearest the injection point benefit first; those farther away feel the increase only when prices have already risen, by which time the new purchasing power has been diluted by the early recipients⁴. The observation later became known as the Cantillon effect. It remains a foundational tool for understanding the distributional consequences of monetary policy, yet rarely appears in mainstream policy discussion.

Under modern financial systems, new money first enters bank reserves and then, through credit expansion, flows toward financial markets and large borrowers. Once commercial banks obtain cheap funding, they preferentially lend to large firms and financial institutions with high credit ratings; those agents convert cheap credit into asset purchases, mergers, or share buybacks. Workers on fixed wages must wait until labor-market tightness feeds into wage growth—a transmission channel that exists, but is lagged and incomplete. Fixed face returns on pension holdings are eroded by inflation; deposit rates typically lag the inflation rate, leaving small savers in a sustained net-loss position.

Data from the Federal Reserve’s quantitative easing between 2008 and 2015 supply the most auditable contemporary distributional evidence chain for the Cantillon effect—to be read together with Section 6 of Chapter 1⁵. Across three rounds of QE the Fed purchased roughly \$3.7 trillion of Treasuries and mortgage-backed securities; its balance sheet expanded from about \$900 billion in 2008 to roughly \$4.5 trillion by early 2015. Long-term rates were suppressed and risk-asset valuations rose systematically. From the March 2009 trough to January 2020 the S&P 500 rose by roughly 400 percent (more on a total-return basis including reinvestment); over a comparable span, Census Bureau figures show real median household income up only about 8 to 12 percent (2019 relative to 2009, with modest variation by inflation-adjustment convention). Correlation is not causation: the easing years also saw profit expansion in technology, a buyback wave, and tax changes; not all of the asset-price rise can be attributed to QE. The testable distributional fact is that the monetary-policy transmission path caused asset prices to respond earlier and more completely to liquidity injections than wages did. The Fed’s Survey of Consumer Finances shows that the top 10 percent of households hold roughly nine-tenths of equity assets—so wealth effects concentrate heavily among those who already held assets, rather than accruing evenly to all holders.

At the institutional level the Cantillon effect produces a systematic political-economy configuration: financial institutions, as direct channels and early beneficiaries of monetary expansion, share common interests with a policy framework that preserves expansionary flexibility. This need not take the form of direct lobbying or corruption; more often it appears as discourse production: frames such as “financial stability,” “employment objectives,” and “preventing deflation” continually emphasize the gains from monetary ease, while distributional consequences are relatively muted as “side effects” or “externalities.” That is an institutional discursive bias; conspiracy theories are unnecessary.

Section 3. The Art of Monetary Communication and the Limits of Forward Guidance

Modern central banks devote substantial resources to “communication policy,” treating it as a core element of the monetary toolkit. In the Greenspan era the Federal Reserve was known for deliberately opaque phrasing (“Greenspan fog”); his successor Bernanke pushed toward more transparent forward guidance, introducing explicit numerical inflation targets and unemployment thresholds. The ECB, the Bank of England, and other major central banks established quarterly inflation reports, press conferences, and economic outlook documents, seeking to amplify policy effectiveness by managing market expectations.

This “communication turn” rests on solid theoretical logic: if market participants can accurately anticipate central-bank actions, price- and wage-setters adjust in advance, reducing short-run pain in transmission. Forward guidance became especially important in the post-2008 zero-interest-rate environment: once rates had reached the floor and conventional cuts were exhausted, “committing to keep rates low for a considerable period” in order to compress the long end became a major unconventional tool.

Yet forward guidance carries an internal tension. To preserve flexibility, central banks typically leave escape clauses in the wording (“data-dependent,” “until ... conditions are met”); that ambiguity in turn weakens the expectations-management effect. If guidance is too precise, any deviation of the economy from the presupposed path creates a public-relations risk of “broken promises” and damages credibility. Orphanides (2003), drawing on Federal Reserve history from the 1960s through the 1990s, showed that even where a clear Taylor-rule-style reaction function existed, actual policy rates often systematically departed from the path implied by the rule—and those departures correlated significantly with subsequent inflation outcomes⁶. In 2021–2022 the Fed labeled inflation “transitory” and maintained an accommodative stance while core PCE rose from about 1.5 percent year-over-year in early 2021 to about 4.7 percent in June 2022, with headline PCE peaking near 7 percent⁷; beginning in March 2022 it hiked continuously, lifting the federal funds target range to 5.25–5.50 percent by July 2023. Markets widely questioned the credibility of guidance after the fact. The episode shows that the value of forward guidance rests on assumptions about central-bank judgment and expectation formation—and judgment is scarce amid supply-chain shocks, fiscal transfers, and energy-price resonance. Misjudgment under a discretionary framework does not automatically imply that “protocol is necessarily superior”; it only shows that constraint vehicles can fail as well, and that comparison must use observable indicators rather than institutional labels.

Section 4. Central-Bank Independence: Myth and Boundary Conditions

The theory of central-bank independence emerged in the 1970s and 1980s against the institutional backdrop of the so-called Great Inflation (roughly 1965–1982): advanced economies endured more than a decade of high inflation, which economists attributed to monetary policy that too readily accommodated short-run political pressure and failed to anchor inflation expectations. In his 1968 presidential address to the American Economic Association, Milton Friedman argued that if a central bank tries to buy employment with inflation, public expectations adjust accordingly and the Phillips curve becomes vertical in the long run—a proposition that supplied important theoretical support for independence and rule-based constraint. The proposed solution was to place monetary authority in an independent technocratic institution, insulated by design from the short political cycle.

New Zealand in 1989 pioneered statutory inflation targeting: the governor bore explicit responsibility for hitting the target and could be replaced for failure—an early attempt to build technocratic accountability into the independence framework. The Bank of England gained operational independence in 1997; the ECB from its inception wrote independence and a clear inflation objective into treaty law, with price stability as its sole primary mandate (unlike the Fed’s dual mandate). Through the “Great Moderation” of the 1990s and 2000s the

arrangement was widely judged a success—inflation in most advanced economies stabilized at low levels, and central-bank credibility earned high marks from markets and the public.

Woodford–Galí models supply a welfare rationale within sovereign fiat systems for an approximately 2 percent target and flexible inflation targeting (FIT): when nominal wages and some prices are downwardly rigid, moderate positive inflation cushions relative-price adjustment and reduces the probability of hitting the effective lower bound (ELB)⁸; FIT also folds the employment gap into the reaction function and claims to have internalized distributional concerns. Within this frame, the book does not urge PCIM to replace the central bank’s full suite of countercyclical tools; it argues for introducing verifiable constraints along the dimensions of mint prerogative and issuance discipline. The 2021–2022 “transitory inflation” misjudgment shows that discretionary frameworks likewise depend on model form and political windows; the debate therefore shifts to “who can independently verify whether constraints are being executed.” On the protocol side, the collateral ratio C_0 , mint/redeem rules, and oracle circuit-breakers are written into a verifiable state machine, so that “covert easing” must occur through visible governance proposals rather than balance-sheet footnotes alone. Blanchard et al. (2010) and Schmitt-Grohé–Uribe (2014) further show that under a more permanent ELB, whether 2 percent remains optimal must be assessed jointly with multiple instruments; optimal policy often must tolerate temporary inflation overshoot. Macroeconomic stabilizers are therefore a multi-instrument problem; a single fixed collateral parameter cannot replicate FIT’s full welfare function—this is a functional division of labor, not a theoretical failure.

The protocol path cannot yet replicate forward guidance or lender-of-last-resort functions under the ELB; actual payment weights and regulatory boundaries still await mainnet and courtroom tests—technical feasibility is not institutional change. Where tax anchors, legal tender, and everyday retail remain dominated by fiat, central banks retain countercyclical tools; in high-friction settings—cross-border settlement, internal pricing within open ecosystems, high-inflation peripheries—verifiable collateral rules may serve as complementary discipline.

Yet “independence” is a matter of degree, not a binary state. Governors are appointed by governments and face reappointment review at term’s end; in extremes, statutes can be rewritten by legislation. Independence rests on political acquiescence, not on constitutional iron law. Between 2019 and 2022 Turkey’s president publicly attacked the central bank’s rate policy, replaced four governors in succession, and repeatedly cut the policy rate even as inflation soared; the Turkish lira depreciated against the dollar by roughly 80 percent from its 2018 peak to its 2023 trough⁹. Central bank of Turkey data show broad inflation repeatedly breaking 80 percent annualized peaks in the same period, while the foreign-currency share of M2 deposits climbed steadily—the aura of the sacred and the tax anchor can coexist in nominal institutions yet fail to halt the collapse of real purchasing power. The case sketches a clear path of eroded independence: administrative pressure to change governors, a policy turn toward lower rates, market responses via depreciation and inflation, with costs ultimately borne by money holders and ordinary citizens.

A more systemic challenge comes from the academic concept of “fiscal dominance”: when public debt is large enough that monetary policy must weigh debt sustainability, a central bank that is nominally independent remains, in substance, fiscally constrained. Canzoneri, Cumby, and Diba (2001) formalized this tension as a fiscal solvency anchor: the price level must be consistent with the long-run solvency of public debt—under an “active fiscal, passive monetary” regime, inflation becomes the equilibrium outlet for debt dilution, running in the same direction as Sargent–Wallace (1981) arithmetic⁶. Bassetto and Messer (2013) further show that although the Fed’s unconventional purchases during the 2008 crisis were operationally independent of the Treasury, they reopened the same debate at the fiscal-sustainability frontier—nominal independence does not equal the absence of fiscal constraint. If rapid rate hikes risk a sharp rise in debt-service costs and a fiscal crisis, will the central bank truly dare to tighten? The Fed’s aggressive hiking in 2022–2023 shows that rapid action remains possible

when inflation clearly overshoots the target; yet those hikes also drove U.S. federal interest outlays sharply higher, planting new pressure on long-run fiscal sustainability—a contradiction that will reappear in new forms in future policy cycles.

Section 5. Political Cycles and the Systematic Bias of Money

The influence of political cycles on monetary policy goes beyond the simple narrative of “incumbents manipulating elections”; it operates through deeper institutional mechanisms. Electoral cycles generate short-horizon pressure: policies whose benefits appear before an election (job growth, rising equities) while costs are deferred (inflation, asset bubbles) enjoy a political advantage over the reverse. Neither corruption nor deliberate manipulation is required; ordinary political rationality alone produces a systematic bias toward monetary expansion.

Public-choice economists Buchanan and Wagner, in *Democracy in Deficit* (1977), joined the policy practice of Keynesian macroeconomics to the incentive structure of democratic politics and argued for a systematic bias toward deficits and inflation under democracy: in booms, raise spending and cut taxes (politically popular); in contractions, raise spending further to stimulate (again popular); austerity is never politically welcome¹⁰. The result is a long-run trend of fiscal deficits and monetary expansion that spans political cycles—less the deliberate act of any single administration than the structural output of institutional incentives.

The logic is not confined to democracies. Authoritarian regimes likewise need to build coalitions and sustain economic performance for legitimacy; monetary expansion remains a low-cost path to resources. The difference lies in constraint mechanisms: democracies in principle have electoral accountability, media scrutiny, and judicial independence; authoritarian systems rely on performance pressure and elite internal checks. Neither regime type is immune to inflation bias; only the forms of expression and the rhythms of eruption differ.

Section 6. War, Crisis, and the Ratchet of the Expansion Threshold

Historically, large-scale monetary expansions have often been linked to war or crisis, and each expansion has somehow widened the practical boundary of monetary policy—once the ratchet turns, return is difficult. Reviewing the history of coinage, Hayek wrote that governments “have incessantly and everywhere abused their trust to defraud the people,” and that only external disciplines such as the gold standard briefly restrained the impulse¹¹—after each crisis, tools once labeled “unconventional” take another step toward the “conventional.”

The gold standard was widely suspended in World War I because wartime financing needs overrode exchange-rate commitments. Postwar efforts to restore it—most famously Britain’s 1925 return at an overvalued parity—ended badly: lost export competitiveness, rising unemployment, and deflationary pressure that forced abandonment again in 1931. That experience was read in the profession as “gold-standard rigidity aggravating the Great Depression,” thereby supplying theoretical support for flexible exchange regimes thereafter. The critique that “the gold standard caused deflation” does not contradict the claim that “the gold standard constrained inflation”—the problem is the bidirectionality of constraint: good constraint suppresses inflation in overheating and offers less stimulative room in contraction. Modern policy preference is for one-way easing flexibility, not symmetric constraint.

The 2008 financial crisis opened institutional space for unconventional tools—quantitative easing shifted from “last resort” to a rapidly deployable conventional option; its distributional consequences are developed along Cantillon lines in Section 2; Sections 3 and 6 of Chapter 1 supply the timeline of balance-sheet expansion and the background of fiscal–monetary symbiosis⁵. Under the 2020 pandemic shock, fiscal transfers and central-bank

bond purchases moved in close coordination; “helicopter money” was in practice implemented in many countries as a “fiscal cash + monetary purchases” package, even though officials rarely used that label directly.

After each crisis, tools once “unconventional” take another step toward the “conventional”: zero rates were an emergency in 2009 and persisted for years in multiple economies through the mid-2010s; between early 2020 and early 2022 the Fed’s balance sheet rose from roughly \$4 trillion to nearly \$9 trillion—a trajectory. The meaning of the ratchet is not only the normalization of tools but the adjustment of policy expectations: market participants begin to price large-scale central-bank intervention as expected, internalize bailout expectations in valuations, and thereby alter risk-taking behavior—laying groundwork for the next crisis.

Section 7. Erosion of the Fiscal–Monetary Boundary and Global Asymmetry

The clearest contemporary expression of fiscal–monetary boundary erosion is the central-bank balance sheet as an extended instrument of fiscal operations—the mechanisms and distributional consequences of QE and primary/secondary-market purchases appear in Section 2 and Chapter 1, Section 6; Chapter 9, Section 4 also treats them from the standpoint of the monetary toolkit. Sargent and Wallace (1981) called the path by which, under high debt, the central bank is forced to accommodate the fiscal authority and dilute debt via inflation “unpleasant monetarist arithmetic”¹²—if a programmable retail CBDC bears interest and has no holding caps, then on Bindseil’s (2024) design discussion that arithmetic may appear still faster on a digital ledger; Kumhof and Noone (2021), in BIS financial-stability design principles, list holding caps, zero remuneration, and reverse waterfall as control devices that lock CBDC into a medium-of-exchange rather than store-of-value role—aligned with Niepelt’s (2024) calibration that “CBDC rates should diverge from reserve rates”¹². These inferences remain provisional; mainnet scale and holding-cap policy still vary by country.

The erosion produces asymmetric effects in the global system. Reserve-currency issuers (chiefly the United States, secondarily the euro area) enjoy “exorbitant privilege” (the famous phrase of former French president de Gaulle): their currencies are held globally as reserves and units of account; the costs and benefits of their monetary policy are distributed worldwide, while decision rights remain concentrated in domestic political-economic logic. Fed rate hikes tighten global dollar liquidity; developing economies face capital outflow, depreciation, and rising external debt service—consequences wholly determined by Fed policy, yet with no formal representation of those external effects in the decision process.

For developing countries, the combination of foreign-currency debt and domestic issuance rights creates persistent tension: when the domestic currency depreciates, the local-currency value of external debt rises and the repayment burden grows; tightening money to stabilize the exchange rate then damages domestic growth; easing to stimulate growth further pressures the exchange rate. This dilemma is known in the literature as “original sin”: unable to borrow in the domestic currency, economies are forced into foreign debt and thus remain weak whichever way exchange-rate and inflation risks move.

“The complicity of inflation and power” therefore has two layers in the global system: domestically, the symbiosis of issuance and fiscal authority; internationally, the structural pressure of reserve-issuer policy spillovers on non-reserve economies. Together the two layers explain why, in the age of globalization, smaller economies often feel a more urgent need for monetary-institution reform.

MMT has explanatory power for sovereign-layer macro space when floating exchange rates, domestic-currency debt, and a reliable tax base are simultaneously present (Wray 2012; Fullwiler 2016 at the operational layer: spending creates reserves, taxes destroy them, Treasuries adjust reserve balances)¹³—yet tax recycling and Treasury reserve adjustment do not automatically imply that “protocol money can never find a foothold”;

competitive on-chain collateralized issuance (PCIM and related design drafts) is a marginal exit option, not a substitute for the macro stabilizer. The fiscal deficits paired with low rates that Sargent–Wallace (1981) foresaw may in the long run be redeemed by an inflationary backlash; in weak institutional environments the value of the protocol path is to offer an exit-capable, verifiable parallel unit of account, not to answer full employment—a judgment awaiting empirical tests of on-chain penetration and tax-anchor division of labor in high-inflation countries (Ma et al. 2023; Eichengreen et al. 2023), not a deduction from white papers alone. Large-scale fiscal–monetary expansion in 2020–2021 and the inflation rebound of 2022 show that inflation constraints are recognized late in politics and that tightening costs are nonlinear—in weak-tax-base regimes such as Turkey, Argentina, and Venezuela, “the real constraint is inflation” quickly shifts from an abstract curve to a lived crisis. MMT’s accounting identities have local truth; they cannot be universalized into a general policy framework. Protocol likewise cannot replace redistributive politics and employment guarantees; popularization expands participation and auditability, not an automatic welfare state. MMT and the protocol path are therefore functionally complementary: the former describes sovereign-layer macro tools; the latter describes auditable issuance discipline in high-friction settings—whether the option exists must be measured by observable indicators such as cross-border remittance shares and the domestic-currency circulation share in high-inflation economies, not by assuming the monopoly is already broken.

Section 8. The Political Economy of Inflation Measurement

Official inflation measurement is itself a policy variable, not a purely neutral statistical activity. Constructing the consumer price index (CPI) requires choosing a basket, defining price-adjustment methods (such as hedonic adjustment for quality improvement), and setting a weighting system—each technical choice has distributional meaning. The housing-cost changes felt by buyers and renters systematically diverge from how “owners’ equivalent rent” is computed in the CPI; the growth of actual outlays by urban wage earners on health care, education, and housing often diverges from the official CPI figure—partly from statistical method, partly from mismatch between basket weights and actual consumption structure.

This does not mean statistical agencies are deliberately fabricating numbers; it means that “inflation” as a single figure is always a compressed simplification of heterogeneous real price changes. The real problem arises when the simplified result is used to set central-bank policy targets: the gap between the conclusion that “the 2 percent inflation target has been met” and some groups’ lived experience of purchasing power becomes a source of eroded monetary-policy credibility. If the tool of “managing expectations”—the official inflation number—persistently diverges from public sensation, expectations management becomes a burden on trust management rather than an aid.

Some economists propose separate “inflation indices” for different income groups to reflect differences in consumption structure—low-income households spend a higher share on food and energy, which often lead inflation cycles. Resistance to such proposals comes partly from statistical complexity and partly from political sensitivity: if officials concede that “the poor experience higher actual inflation,” the distributional bias of monetary policy becomes an unavoidable public topic rather than a footnote in academic papers.

Section 9. Fixed Rules as Constraint: Historical and Modern Options

Confronting the systematic complicity of inflation and power, the history of economic thought developed a tradition of substituting fixed rules for discretion. In the 1960s Milton Friedman proposed a “constant money-growth rule”: the central bank should expand the money supply at a fixed rate (roughly 4 to 5 percent per year), undisturbed by cyclical conditions. Operationally the proposal ran into unstable money demand, yet the

institutional logic behind it—constraining discretion and shrinking the space for political intervention—represents an important path in monetary thought.

Gold-reserve rules were historically the longest-lived form of fixed rule: while a standard operated, the quantity of money issued was anchored to deliverable commodity, and the cost of violation was conversion pressure and reputational loss. The limitations were the geographic contingency of gold supply and the procyclical risk of deflation—gold output and the monetary needs of growth did not match; booms lacked adequate monetary lubrication, and contractions lacked countercyclical buffers.

Blockchain protocols push rule constraint onto a new technical plane: as white papers envision, supply caps and issuance schedules can be written into code; post-deployment changes require consensus among a majority of network participants, and no single issuer can unilaterally amend them—the analogy to the gold standard holds at the level of mechanistic design: both use external constraint to limit the unilateral incentive to expand issuance. Hayek held that fixed convertibility obligations such as the gold standard “provided the only discipline that effectively prevented monetary authorities from giving in to the demands of the ever-present pressure for cheap money”¹⁴, yet their force was ultimately broken by politics—the observability of code constraints and the cost of forks supply an external discipline of a different kind. Rules can be encoded and state audited; that much is already technically feasible. Mainnet scale, regulatory access, and tax anchors remain heavily skewed toward fiat; hard forks and governance failures can rewrite rules as well (Terra/UST and several 2022 governance events are counterexamples)—these must be stated separately. The difference is this: gold’s constraint comes from physical scarcity; code’s constraint comes from social consensus (holders who reject a rule change fork and preserve the value of the original chain)—the latter can be overturned in extremes, but the cost of overturning is observable; observability is not occurrence, and so the claim can be stated only as a possibility, not as an established institutional fact.

Code constraint and gold constraint are not equivalent, and monetary problems cannot all be handed to rules. The limit of rules is that they handle constraints that can be formalized and cannot handle emergencies outside their scope. Good institutional design must hold tension between rule constraint and emergency flexibility, rather than eliminate one side entirely; protocol design must face that tension rather than choose only one.

Historical experiments with rule constraint offer details worth consulting. The Bretton Woods gold-exchange standard was a hybrid in which the United States bore convertibility obligations and other countries held dollars as reserves—not a full gold standard. Its fragility lay in the fact that enforcement ultimately depended on U.S. willingness and capacity, not on a truly automatic mechanism. Nixon’s unilateral decision in 1971 broke the surface constraint of that “rule.” By contrast, Bitcoin’s 21-million supply cap under current mainnet consensus depends on no nation’s will—no sovereign can unilaterally announce a “pause of the cap” and expect the network to continue under the old rules; yet if the holder community accepts new rules via hard fork, the constraint can likewise be rewritten, only with publicly observable cost and process. Turning a technical scheme into social consensus still requires time and observable adoption—tests must refer to on-chain payment volume, fiat tax anchors, and similar indicators.

Monopoly mint prerogative has played a real positive role in lowering transaction costs and expanding market coverage; once monopoly hardens, however, institutional incentives continuously point toward expansion. The complicity of inflation and power is a product of incentive structure, visible alike in democratic and nondemocratic, developed and developing economies—differences lie only in forms of expression and rhythms of eruption. That holders cannot verify issuance rules, that issuance channels concentrate in few hands, and that

monetary policy lacks auditable transparency—these three point to different repair directions and must not be conflated.

These mechanisms operate on different time scales: the benefits of the inflation tax arrive over months to years; full Cantillon transmission takes years to a decade; political-economy bias is a multi-decade trend. Within a single political cycle they often register as hard-to-attribute “background noise” rather than clear political scandal—one reason the complicity can cross eras. Under monopoly issuance, external constraint—commodity anchors, institutional independence, or publicly verifiable protocol rules—is not a superfluous ideal but a practical need to check over-issuance.

注释与引用

1. Hayek (1976), *The Denationalization of Money*, p. 69: “Successful calculations, or effective capital and cost accounting, would then become impossible.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
2. Keynes (1923), *A Tract on Monetary Reform*, ch. 1 “The Consequences to Society of Changes in the Value of Money”: “by a continuing process of inflation, governments can confiscate, secretly and unobserved, an important part of the wealth of their citizens.” Project Gutenberg public-domain text: <https://www.gutenberg.org/ebooks/6778> ↩
3. Mises (1912), *The Theory of Money and Credit*, Liberty Fund 1980 ed., p. 240: “an increase in the quantity of money (in the broader sense of the term, so as to include fiduciary media as well), that is not offset by a corresponding increase in the need for money ... so that a fall in the objective exchange value of money must occur.” English translation: <https://www.econlib.org/library/Mises/msT.html> ↩
4. Cantillon (c. 1730), *An Essay on Economic Theory*, ch. 7, pt. 2: after money is injected into the economy it “cannot augment the real quantity of industry ... in equal proportion to the quantity of money added”—new money is distributed unevenly along the path, and those nearest the injection point benefit first. Liberty Fund English translation: <https://oll.libertyfund.org/titles/cantillon-an-essay-on-economic-theory> ↩
5. Federal Reserve H.4.1 balance sheet: three rounds of QE purchased ~\$3.7 trillion cumulative (Bernanke 2015 retrospective); Aug. 2008 ~\$908 billion → Jan. 2015 ~\$4.5 trillion. S&P 500: close 676.53 on 2009-03-09 → ~3329 on 2020-01-17 (Yahoo Finance / FRED SP500 series, ~392% gain); total-return basis higher. Real median household income: Census Bureau *Historical Income Tables* F-5/F-6, 2009→2019 ~+8%–12% (2019 dollars). Top 10% equity holdings: Fed SCF 2022, top 10% hold ~87%–93% of equity wealth. Correlation ≠ causation as in the text. ↩ ↩²
6. Orphanides (2003), “The Quest for Prosperity Without Inflation,” *Journal of Monetary Economics* 50(3), pp. 715–730 (1960s–1990s Taylor-rule historical deviations and inflation consequences); Canzoneri, Cumby & Diba (2001), “Is the Price Level Determined by the Needs of Fiscal Solvency?,” *AER* 91(5), pp. 1221–1238 (fiscal solvency anchor; read with Leeper 1991); Bassetto & Messer (2013), Chicago Fed WP 2013-13, pp. 1–35 (Fed unconventional operations and the fiscal boundary in the crisis). [https://doi.org/10.1016/S0304-9332\(03\)00028-7](https://doi.org/10.1016/S0304-9332(03)00028-7) ; <https://doi.org/10.1257/aer.91.5.1221> ; <https://doi.org/10.21033/wp-2013-13> ↩ ↩²
7. Federal Reserve FRED series PCEPILFE (core PCE): 2021-01 ~1.5% y/y → 2022-06 ~4.7%; PCEPI (headline PCE) 2022-06 ~6.8%–7.0% y/y. Federal funds target range raised from 2022-03 to 2023-07 5.25%–5.50% (FOMC statements). “Transitory” phrasing: Powell 2021-06-16 press conference transcript. ↩
8. Woodford (2003), *Interest and Prices*, ch. 6 (pp. 235–280, nominal rigidities and optimal inflation), ch. 7 (pp. 281–330, ELB); Galí (2015), *Monetary Policy, Inflation, and the Business Cycle*, 2nd ed., ch. 8 (pp. 145–180), ch. 15 (pp. 320–340, FIT and discretion–commitment trade-offs); Blanchard, Dell’Ariccia & Mauro (2010), IMF SDN/10/03 (whether 2% remains optimal under the ELB); Schmitt-Grohé & Uribe (2014), *AER* 104(5) (multi-instrument joint policy and inflation overshoot under the ELB). Welfare proofs depend on specific model parameters and are not universal theorems. ↩
9. Turkish lira USD/TRY: 2018-08 ~4.7 → 2023-06 ~26 (TCMB / FRED DEXTRYUS), cumulative depreciation ~80%+; CBRT inflation and foreign-currency deposit share of M2: Central Bank of the Republic of Turkey monthly statistics. ↩

10. Buchanan & Wagner (1977), *Democracy in Deficit*, ch. 1 (incentive mismatch between democratic politics and Keynesian policy practice), ch. 2 (systematic deficit bias): “the political process ... generates a bias toward deficit finance”—raise spending and cut taxes in booms, stimulate again in recessions; austerity is politically unwelcome. <https://doi.org/10.1016/B978-0-12-139250-3.50008-5> ↩
11. Hayek (1976), *The Denationalization of Money*, pp. 30, 35: government coiners “have incessantly and everywhere abused their trust to defraud the people”; the gold standard “imposed ... a discipline” that for a time restrained over-issuance. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
12. Sargent & Wallace (1981), “Some Unpleasant Monetarist Arithmetic,” *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1981, pp. 1–17: under high fiscal deficits, if the central bank tries to accommodate fiscal policy with low rates, higher inflation must eventually redeem the arithmetic; Bindseil (2024), ECB OP 322, §§5–6 (payment-type vs. investment-type CBDC, holding caps); Kumhof, Michael & Clare Noone (2021), “Central bank digital currencies — design principles for financial stability,” BIS WP 880, §§3–5 (holding caps, zero remuneration, and financial stability); Niepelt (2024), “Money and Banking with Reserves and CBDC,” *Journal of Finance* 79(4), pp. 2505–2552 (optimal divergence of CBDC and reserve rates). <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ; <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op322~5822218919.en.pdf> ; <https://www.bis.org/publ/work880.htm> ; <https://www.niepelt.ch/files/jf2024.pre.pdf> ↩ ↩²
13. Wray (2012), *Modern Money Theory*, ch. 2 (taxes create demand for domestic currency), chs. 5–6 (fiscal space); Fullwiler (2016), Levy WP 855 (spending creates reserves, taxes destroy them, Treasuries adjust balances); Sargent & Wallace (1981), “Some Unpleasant Monetarist Arithmetic”; Ma, Ye, Yan Ji, and Andreas Schrimpf (2023), IMF WP 23/72 “Stablecoin Flows and Crypto Markets”: stablecoin flows under stress; Eichengreen, Gupta & Masucci (2023), IMF WP 23/110: emerging-market corridor adoption. ↩
14. Hayek (1976), *The Denationalization of Money* (revised ed.), p. 108: fixed convertibility obligations “provided the only discipline that effectively prevented monetary authorities from giving in to the demands of the ever-present pressure for cheap money.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩

Part II: Ideas and Competition

§ 4 The Theory and Dream of Competing Currencies

The collusion of inflation and power puts on the table the question of who pays for monetary dilution; from that diagnosis Hayek advanced the idea of competing currencies.

Monetary monopoly was never inevitable, and doubts about it have never fallen silent. Across the history of economic thought, calls to open currency issuance and introduce competition have appeared in different guises: from nineteenth-century advocates of free banking, through the institutional economics of the Austrian school, to Hayek's systematization of the idea as a policy proposal in the 1970s. When *The Denationalization of Money* appeared in 1976, it met almost no response; half a century later, the rise of blockchain technology brought it back into view as one of the principal coordinates for understanding contemporary monetary change. The idea of competing currencies has a theoretical logic, historical practice, and structural limits; it need not be read as a classic text to be refuted point by point, but as a series of unfinished questions.

Section 1. Hayek's Core Questions and Epistemological Foundations

Throughout his scholarly career Hayek held a deep and systematic belief in the price mechanism: market prices are not merely signals for resource allocation, but a system for transmitting dispersed knowledge. No single actor—whether a government agency or a private firm—can command information complete enough to replace market prices; the function of competition is not only “efficiency” but also “discovery”—the discovery of previously unknown preferences, techniques, and combinations. This epistemological stance runs through his critique of planned economies (*The Road to Serfdom*, 1944) and his elaboration of spontaneous order (*Law, Legislation and Liberty*, 1973–1979), and finally extends into the monetary domain.

In *The Denationalization of Money* he noted an asymmetry: markets for goods and services rely on competition to discover quality and price, yet the monetary sphere has long been excluded from competition by sovereign monopoly. The monopolist lacks an external incentive to maintain the value of money—because the public has no substitute with which to “exit”—yet enjoys a continuing convenience in financing the fisc through monetary expansion. Hayek wrote: “Good money can come only from self-interest, not from benevolence”¹—competition forces issuers to trade currency stability for survival, just as product markets trade quality for customers. His proposal was to open the right of note issue, allow private institutions to issue named currencies on their own reputation, and let the public, through use, choose units of more stable purchasing power, so that competition would weed out inferior issuers and retain superior ones.

That question remains powerful: if issuance rules can be manipulated, why should holders not seek alternatives? If price competition works in goods markets, why should money markets be the exception? The theory of dispersed knowledge that Hayek developed in *Individualism and Economic Order* runs through this argument: “the function of competition is not only efficiency but discovery”—no single actor holds information complete enough to replace market prices². The logical chain of these two questions is intact—yet Hayek's epistemological premises also include an important assumption: for competition to work effectively, several conditions must be met, including accessible information, acceptable switching costs, and credible constraint mechanisms. In the nineteenth and twentieth centuries, when metallic money and paper notes coexisted, the supply of these conditions was scarce, and the idea of competing currencies accordingly remained largely theoretical. The key is what infrastructure competition requires, not an abstract debate over whether competition is wanted.

Section 2. Historical Practice of Free Banking: Scotland's Positive Case

The main historical empirical basis for free-banking doctrine comes from Scotland's experience between 1716 and 1845. In that period, Scotland's money and credit were supplied mainly by competing private banks; the Bank of England's charter did not extend to Scotland; each bank issued notes backed by its own reputation and accepted one another's paper under spontaneously formed multilateral clearing arrangements.

The record of this history is largely favorable. Economic historian Lawrence White, in *Free Banking in Britain* (first edition 1984), systematically surveyed the evidence: Scottish banks showed lower failure rates than their English contemporaries, broader financial coverage (including deposit services for urban and rural small savers), and more stable monetary quality. Scottish banks developed an "option clause" allowing a bank under liquidity pressure to postpone specie redemption for six months while paying 5 percent compensatory interest—a spontaneous liquidity-management device that did not depend on any government lender of last resort³. Selgin's evolutionary model of competitive note issue, published the same year, embedded this mechanism in a dynamic path of "overissue—discount—clearinghouse reflux," laying the framework for his 1988 monograph³.

White's positive narrative is only one wing of a long historiographical debate, far from scholarly consensus. George Selgin, in *The Theory of Free Banking* (1988), derived monetary-supply discipline from a model of competitive issue: absent an artificially fixed parity, overissued notes would trade at a discount in the exchange market, and the public would spend discounted notes first and hold superior ones—aligned with Thiers' law in Chapter 5, except that the mechanism shifts from national exchange rates to interbank clearing and discount rates⁴. In *How Would the Invisible Hand Handle Money?* (1994), Selgin and White argued further that clearinghouses, option clauses, and peer monitoring could endogenize stabilizing mechanisms so that competitive issue need not inevitably produce hyperinflation.

Critics do not deny that Scottish banks were relatively prudent; they question causal attribution. Charles Calomiris has pointed out that the Scottish system operated in the shadow of the British gold standard and the Bank of England as lender of last resort; in crisis years (such as 1825 and 1837) it often relied on London liquidity support. Strip away England's institutional background, and the evidence that "pure competition" could be replicated is insufficient⁵. White responded directly in 1995: Scottish banks' lower failure rates relative to English contemporaries cannot simply be attributed to an "English backstop," but must be read as the joint product of clearing networks, option clauses, and community reputation constraints—yet even White conceded that counterfactual experiments fully stripped of the national gold-standard framework cannot be supplied by the sources⁵. Surveying the debate, Randall Kroszner acknowledged that the Scottish experience is instructive for understanding competitive issue, but that extrapolating it directly to contemporary emerging economies requires careful distinction among community scale, legal enforcement, and clearing infrastructure⁶. Warren Weber, in a Minneapolis Fed quarterly review, further summarized: the Scotland–United States contrast turns not on the labels "free / unfree," but on three institutional variables—bond-collateral rules, branching rights, and note-authentication costs—narratives that can be read alongside Calomiris's political-bargain explanation and Selgin's endogenized-clearinghouse explanation rather than canceling one another⁷. Kevin Dowd showed from the modeling side that, within a competitive-issue framework, clearinghouse networks can endogenize "overissue—discount—reflux," so that supply discipline need not depend on a single central bank—yet model conclusions likewise depend on whether clearing rules are enforceable and whether participants cannot escape discounted clearing⁸. Hugh Rockoff's reexamination of the American free-banking era provides another mirror: failure rates under state "free banking" laws varied enormously and were not sheer chaos—institutional detail (especially reserve and bond-collateral rules) often mattered more for outcomes than "whether banking was free"⁹.

In a 1986 reappraisal of the legal-restrictions theory of money, Selgin offered a third reading: many “failures” of the American free-banking era were not necessarily deteriorations of competition itself, but layered legal restrictions—bans on interstate branching, compulsory state-bond collateral for notes, and the post-1865 holding tax on state banknotes—that successively blocked the discount clearing and Thiersian direction the market might otherwise have supplied¹⁰. This “legal restrictions theory” and the Calomiris–Haber political-bargain explanation are not mutually exclusive: the former asks which rules structurally distort relative prices; the latter asks who profits from the rules. Read together, they show that before opening competition one must clarify whether the restriction list can be removed, and whether after removal information costs remain high enough to require a clearinghouse or an on-chain state machine. When Hayek reviewed parallel-currency experience in Chapter 7 of *The Denationalization of Money*, he drew mainly on continental European cases; had he encountered Selgin’s historiographical reconstruction of the 1865 federal tax and the legal-restrictions framework, he might equally have stressed that whether competition can discover discipline depends on whether relative prices can adjust with the market—aligned with the Thiersian reading in Chapter 5 and the Hayek Gresham/Thiers boundary in Section 7 of Chapter 7.

In a 1991 *Cato Journal* essay, “The Case for Free Banking: Then and Now,” Selgin moved the historiographical debate from “whether Scotland succeeded” to a list of institutions transferable to the present: for competitive issue to discover discipline, it must simultaneously satisfy (1) notes circulating at market discount rather than forced parity; (2) branching and clearing networks sufficient to reflux overissue; and (3) a legal-restriction list that can be identified and removed—rather than an a priori claim that “private issue is necessarily chaotic”¹¹. In *Competition and Currency* (1989), White further brought another internal free-banking-school disagreement onto the table: some in the Austrian tradition (such as Rothbard) held that only 100 percent reserves count as “non-fraudulent issue,” whereas White and Selgin argued from Scottish sources that fractional reserves plus clearinghouse discipline were, in the nineteenth century, a workable and relatively prudent institutional combination—the dispute focusing not on “whether competition is wanted,” but on how reserve rules and clearing constraints are paired within a competitive framework¹¹. In dialogue with Hayek, this internal disagreement is worth retaining: Hayek wanted competition to discover discipline and did not lock in a single reserve ratio in *The Denationalization of Money*; Scotland’s option clauses and clearinghouse networks show that discipline can be embedded in interbank rules, not only in 100 percent metallic backing. In the on-chain era, MakerDAO-style overcollateralized CDPs and the dynamic-tier overcollateralization of VRC-10/PCIM (circulation thresholds triggering public votes, with an upper tier near 161.8%) functionally approach a modern variant of “verifiable reserves plus automatic redemption/liquidation”—whether superior to nineteenth-century paper clearinghouses must be tested by peg-deviation and run-recovery data, not decided a priori by historiographical allegiance.

In dialogue with Hayek, the foregoing debates should be read as different facets of the same question, not as taking sides on whether free banking is “good” or “bad.” Hayek wanted competition to discover discipline; Selgin and White show that discipline can be partly endogenized in banking networks; Calomiris and Rockoff remind us that discipline also depends on clearing arrangements, lender-of-last-resort expectations, and judicial enforceability—conditions that in 1976 could scarcely be replicated globally by private institutions. A more cautious reading is that the Scottish case shows under particular community conditions reputation competition can work, but it does not prove that reputation alone suffices in anonymous global markets; verifiable on-chain rules fill a gap in identification costs, without denying the critics’ empirical grounds in the historiographical debate.

That the Scottish case could operate was closely tied to several specific conditions. The Scottish banking community was relatively small; bankers were highly visible within commercial circles, and the consequences of reputational loss were direct and palpable; competitive clearing agreements among multiple banks formed spontaneously, reducing interbank frictions; and the legal system supplied reliable contract enforcement. That combination made reputation competition genuinely effective at a local scale.

Yet the Scottish case cannot simply be copied. It was an experiment within a geographically limited, economically tightly linked, culturally proximate community; information asymmetry between holders and issuers remained manageable because Scotland was not large and bank information was relatively transparent. Once the model is scaled to anonymous, globalized mass markets, the effectiveness of reputation mechanisms faces structural pressure.

Section 3. Adam Smith, Ricardo, and the Historical Genealogy of Competing-Currency Thought

Before Hayek, competitive ideas in the monetary domain were not without precedent. In *The Wealth of Nations* (1776), Adam Smith did not give unconditional support to monetary monopoly. He observed that the higher degree of competition in the Scottish banking system relative to England helped promote prudent management; he favored banks' issuing paper under adequate reserves to raise capital efficiency, holding that competition led banks to curb excessive credit. Yet Smith also supported minimum-denomination limits on certain note issues, arguing that if very small notes were held largely by the poor, bank failure would impose unfair losses. That stance foreshadowed a lasting tension in competing-currency discussions: competition benefits large holders able to assess risk, while small depositors facing greater information asymmetry may suffer asymmetric losses.

On monetary questions Ricardo leaned more toward rule-based approaches. In *The High Price of Bullion* (1810), he argued that paper exceeding the quantity needed for gold circulation would depreciate, and favored constraining issue by a commodity standard to prevent banks' excess money creation. His "quantity theory of the currency" became a foundation for the later Currency School and influenced the Peel Act of 1844—which separated the Bank of England's Issue Department from its Banking Department and capped note issue by a forced reserve ratio. The nineteenth-century debate between the Currency School and the Banking School (which held that credit should respond flexibly to economic demand and not be bound by hard commodity reserves) was in substance an early clash between two philosophies of monetary management—"rule constraint" and "discretion." That clash continues in different forms today—debates between Keynesian monetary policy and the Austrian school, between central-bank independence and fiscal dominance, between code rules and governance flexibility, are all modern variants of this older opposition.

Recognizing this historical genealogy helps avoid two extremes: one cannot simply assert the absolute superiority of on-chain rules because "rule constraint has historical precedent," nor deny the value of rule constraint because "rules have historically been broken." The real lesson of monetary intellectual history is that rule constraint and flexibility must be balanced within concrete institutional frameworks, and that different technical conditions shift the feasible boundary of that balance.

Section 4. The American Free Banking Era: Chaos and Learning

In sharp contrast to the Scottish case stands the American "Free Banking Era" of 1837–1863. After the federal government failed in 1836 to renew the Second Bank of the United States' charter, states legislated

banking for themselves; most allowed any institution meeting minimum capital requirements to obtain a bank charter and issue notes.

The result was a flood of notes, numerous but uneven in quality. By 1861, notes in circulation came from more than 1,500 different banks¹², with exchange rates floating by each bank's reputation; discounts might range from 1–2 percent (reputable big-city banks) to 100 percent (banks already failed or unable to redeem)—Rockoff derived this order of magnitude from state circulation statistics and discount ranges compiled in the *Bank Note Reporter*⁹. Bank-note reporters arose so that merchants could judge the actual value of notes in hand—a market's spontaneous response to information asymmetry, yet also evidence of how high competition's transaction costs could be: in an age without real-time verifiable ledgers, “open competition” and “low-information-cost competition” were not the same thing.

Rockoff's research on the period revises the popular narrative of “wildcats everywhere and total failure”: free-banking statutes differed sharply across states; some (such as New York and Ohio) used bond collateral and supervisory clauses to hold failure rates within acceptable ranges, while others permitted overissue⁹. The National Banking Acts of 1863–1865 imposed a 10 percent holding tax on state banknotes; drawing on issue statistics and discount series, Selgin argued that the tax effectively prohibited state notes from circulating at a discount and gave national banknotes a de facto legal parity—blocking the Thiersian direction so that, after the Civil War, private notes nearly vanished from circulation¹³. This institutional intervention is often overlooked, yet it shows that the endpoint of “open competition” can be legislative reconstruction of parity rather than natural market convergence; parity laws and federal tax suppression show that Gresham's mechanism can be re-embedded in private systems by legislation.

This contrasts with the Scottish debate—whether competition “works” often depends on accompanying clearing and asset-constraint rules, not on abstract slogans. When Hayek discussed parallel-currency experience in Chapter 7 of *The Denationalization of Money*, he drew mainly on continental European and Latin American cases; had he encountered Rockoff's empirics on interstate institutional variation and Selgin's reconstruction of the 1865 suppression, he might equally have stressed that before opening competition one must answer “who executes clearing and constraint, and how is it verified”—the same set of institutional questions posed by verifiable rules.

So-called “wildcat banks” became the period's most famous negative cases: banks located their headquarters in remote, hard-to-reach places to reduce actual redemption requests while circulating large volumes of notes in distant cities. When holders tried to redeem, they might find the headquarters “in wildcat country,” or find that the bank lacked sufficient reserves. Dwyer, drawing on state charter geography and *Bank Note Reporter* discount records, showed that the wildcat structure was essentially arbitrage on authentication and redemption costs—the surface result sometimes resembled Gresham-style retention of bad notes, yet the trigger was information cost rather than legal parity¹⁴. Under weak reputation constraints, such institutions extracted considerable short-run seigniorage, the cost borne by uninformed note holders.

The Panic of 1907 displayed the systemic fragility of a banking system lacking central-bank liquidity support: the federal Free Banking Era had ended in 1863, yet under the National Banking Acts there was still no central bank as lender of last resort; interbank runs spread rapidly and were finally calmed only by JP Morgan's privately organized rescue. That episode directly propelled the creation of the Federal Reserve System in 1913—driven less by abstract monetary theory than by repeated demonstration that in the absence of a lender of last resort, private banking networks still face contagious runs. The historical roots of government intervention

therefore include, alongside “desire for power,” institutional responses to real market failure; yet 1907 should not simply be attributed to the free-banking experiment of 1837–1863 itself.

Section 5. The Technical Conditions Competition Requires

Hayek’ s scheme implied several critical technical premises that his era could not satisfy—key to understanding why the proposal was hard to implement at the time. The competitive path he envisioned was that countries would open monetary competition to one another and “impose upon existing monetary and financial agencies a very much needed discipline”—any issuer departing from honest money would see its currency rapidly displaced¹⁵—yet without real-time verifiable ledgers, that discipline was hard to land.

Identifiable and comparable issuance rules are the first condition. If holders cannot readily learn a currency’ s issuance rules and reserve position, they cannot make meaningful comparative choices. Traditional banks disclose balance sheets quarterly or annually; the information is delayed and requires professional interpretation. Competing currencies need real-time accessible rule descriptions and state verification.

Low switching costs are equally indispensable. If moving from currency A to currency B requires lengthy account opening, approval procedures, and high fees, holders will inertially keep their current choice even when theoretically superior substitutes exist. Network effects are extremely strong in money; when switching costs are high, market response is slow even when gaps are clear.

Enforceable constraints and default penalties form the third. If an issuer advertises stability while actually expanding, holders must be able to verify and sell at low cost, and exit itself must send a strong enough punitive signal to discipline future issuance. In dispersed, information-asymmetric markets, this requires high-frequency price discovery and low liquidity frictions.

None of these three conditions could be met at low cost in the 1970s; Hayek’ s vision was therefore more a thought experiment than a practical policy roadmap. In Chapter 22, “The Problem of Transition,” he conceded that abolishing legal tender overnight and fully opening competition was almost politically and contractually infeasible; the revised edition also admitted the scheme might be “too radical”¹⁶—the political feasibility of transition is a fundamental obstacle, not one solvable by technical detail alone. Transition is better understood as marginal substitution rather than overnight institutional switching, in keeping with that spirit.

Technical change has altered the supply possibility of these conditions: blockchain networks make issuance rules and ledger state, in principle, globally and in real time inspectable (identifiability); standardized interfaces (ERC-20, VRC-20, and the like) compress code-layer switching frictions (comparability); MakerDAO-style CDP automatic liquidation auctions and on-chain liquidity pools bring price discovery near continuous (punishability); VRC-10/11 risk paths are set out in the glossary. Most wages, taxes, and legal tender remain tied to sovereign money; deployable on-chain tokens are not the same as clearing licenses and compliant access (for on-chain real-payment metrics, see Chapter 1, Section 8¹⁷). Hayek’ s vision of “bad money rapidly displaced” is more likely today to occur first in high-friction edge cases (cross-border remittance, high-inflation store of value, open-ecosystem internal pricing) than overnight rewriting of everyday settlement networks in advanced economies.

Section 6. Reputation, Rules, and Verifiable Constraints

The core mechanism of competing-currency theory is reputation competition: issuers discipline themselves to maintain market value; holders punish the untrustworthy by selling. The mechanism can work effectively in markets with adequate information, dispersed and highly mobile holders—substituting continuous market discipline for ex ante regulatory approval.

Yet reputation mechanisms have two structural weaknesses in the monetary domain. Information lag comes first: an issuer's internal condition cannot be observed in real time, and manipulation can be completed before disclosure. The 2022 collapse of FTX is a clear case: the platform had a strong reputation; its founder was widely seen as a responsible industry builder; until days before failure, many analysts still gave positive ratings. Reputation could not prevent internal diversion of customer funds, because the diversion was invisible from outside. Reputation's limit is that it is a lagged function of outcomes, not a leading indicator.

"Too big to fail" expectation distortion is the other. When an issuer grows large enough that failure would trigger systemic contagion, the punitive function of reputation is diluted by expectations of government bailout—holders expect government not to allow failure and therefore lower their self-protective vigilance. This is a classic form of moral hazard; in crypto it appears in a slightly different guise: government bailouts become "consortium rescues" and "protocol restarts," which can likewise dilute market discipline.

In the on-chain era, rule constraints partly substitute for reputation constraints: supply caps, public collateral ratios C_0 , Maker-style CDP automatic liquidation thresholds, and issuance schedules are written into code and cannot be unilaterally changed after deployment. This shifts the question "does the issuer keep faith?" from dependence on disclosure and reputational appraisal to dependence on code verifiability—anyone can read the contract code, confirm that rules match advertising, and see that rules cannot be modified without broad social consensus. Timberlake showed from nineteenth-century clearinghouse sources that the paper-era prototype of "verifiable discipline" was already the reflux of discounted notes onto overissuing banks by interbank clearing networks—full on-chain nodes continue the same logic structurally, only the medium shifts from clearinghouse books to a state machine¹⁴. Reputation and verifiable rules are complementary, not substitutes: code handles constraints that can be formalized; reputation handles flexibility and judgment beyond the code's boundary.

Section 7. The European Monetary Union: A Counter-Experiment in Competition

In the revised edition of *The Denationalization of Money*, Chapter 1, "A Realistic Proposal," Hayek proposed that a near-term operable first step would be for Common Market countries, by treaty, to remove barriers to currency flows and cross-border banking, allowing national currencies and banks to compete freely within each territory—preferable to the "utopian scheme" of issuing a common European currency¹⁸. History moved in the opposite direction: Europe chose a single currency. The Maastricht Treaty of 1992 set the course; the euro launched as a unit of account in 1999; euro notes and coins entered circulation in 2002; twelve founding members abandoned their own currencies. Competitive weeding-out did not occur; the euro came from political negotiation, aimed at eliminating exchange-rate frictions and lowering cross-border transaction costs, advancing European political integration through monetary union.

Euro-area experience supplies a complex reference for competing-currency theory. Monetary unification did lower transaction costs among members: Eurostat data show that in the euro area's first decade, intra-area goods trade as a share of intra-EU trade rose from about 45 percent to a peak near 67 percent around 2007¹⁹—eliminating exchange-rate frictions brought a quantifiable trade-integration effect. Unified market scale also briefly brought the euro's share of global foreign-exchange reserves near 30 percent in the 2000s, rivaling the dollar¹⁹. Yet by abandoning exchange-rate policy tools, members facing asymmetric shocks lacked independent adjustment means. In the sovereign-debt crisis of 2010–2015, Greece, Spain, and Portugal could not restore competitiveness through domestic-currency depreciation and had to rely on painful internal price and wage adjustment. Thomas Sargent, in his Nobel lecture, characterized the euro-area debt crisis as "the inevitable

tension of incomplete fiscal-union design inside a monetary-union shell”—without adequate fiscal-transfer mechanisms, monetary unification under asymmetric shocks generates large distributional pressures.

From the standpoint of competing-currency theory, the euro-area experiment shows that eliminating monetary competition (substituting political unification for market competition) does not dissolve the core problem of seigniorage—incentive structures and constraint mechanisms do not vanish when names are unified; they reappear in new forms. Southern European countries within the euro area could not lighten debt burdens through currency depreciation; the result was sovereign-debt crisis. Had those countries retained independent currencies, similar pressures would have been released through depreciation plus inflation, the cost borne by money holders. Both paths have costs; the difference is who bears them and in what form. That is highly consistent with Hayek’s core claim—that monetary problems are essentially distributional questions of who bears the cost.

Section 8. Mises’ s Monetary Theory and the History of Parallel Currencies

Ludwig von Mises was Hayek’s teacher and another major Austrian voice on monetary theory. His “regression theorem” sought to explain the origin of money’s value: money’s present purchasing power rests on people’s expectations of its historical purchasing power, which can be traced back to the point at which money, as a commodity, had use value²⁰. Some scholars have used the theorem to argue that Bitcoin cannot be money—without an original commodity use value, how can value have an initial anchor?

In “Synthetic Commodity Money” (2015), Selgin proposed a path that dialogues with rather than denies the regression theorem: Bitcoin can be seen as a “synthetic commodity”—scarcity, verifiability, and censorship resistance substitute for metal’s physical properties, so that it functionally takes on the constraining role commodity money once provided²¹. This sits closer to Menger’s logic of “saleability”: markets select attribute combinations that lower exchange frictions, not necessarily some predetermined “nonmonetary use value.” In practice, Bitcoin has sustained market capitalization and trading for more than fifteen years; the theorem’s relation to that fact is more a matter of historical origins and epistemology than functional negation—how a zero price on day one is anchored, and how continuous quotation on year fifteen is maintained, are two different layers. Had Mises seen this outcome, he might have distinguished “the regressive chain of explanation” from “saleability ranking under institutional competition,” rather than using an origin theorem to deny a continuing market fact—consistent with the Austrian school’s habitual pragmatism.

Of greater practical reference is Mises’s historical analysis of parallel currencies. He observed that historical coexistence of multiple monies was not naturally chaotic—so long as an expectable relative-price mechanism exists, multiple currencies can serve different scenes and functions without necessarily producing economic disorder²². The key is not “whether multiple currencies exist,” but divergence between officially fixed parities and genuine market valuations—that is the trigger for Gresham’s law, bad money driving out good. Under freely floating exchange rates, markets continually adjust relative prices among currencies, maintaining a dynamic balance that differs in kind from static pricing under monetary monopoly.

Section 9. Two Unresolved Problems of Competing Currencies

Hayek’s competing-currency scheme left two theoretical problems that remain incompletely answered and must still be faced.

Scale effects and new monopolies form the first tension. Competing-currency theory assumes market selection will preserve a plural pattern; yet network effects in money are extremely strong—money’s value derives partly from general acceptance, and acceptance rises with scale of use. Competition may therefore produce not a stable plural pattern but a winner-take-all new monopoly. Experience from internet platform

economies suggests that competition's result is not always plural coexistence; first-mover advantage plus network effects can quickly yield dominance. In money, the logic that "scale is value" continually strengthens the first currency to win broad adoption, while later entrants face extremely high network thresholds. If ultimately only one private money dominates, the discipline competition brought disappears, and the outcome may be no better than regulated central-bank money.

Deflationary bias and macro stability form the second tension. Issuers of competing currencies, to maintain purchasing-power stability, naturally avoid overexpansion—rational at the individual-incentive level. But if all issuers lean toward conservative supply policy, aggregate money supply lacks elasticity in economic contraction and may intensify deflationary pressure—the core of Keynes' s critique of the gold standard. Del Negro, Giannoni, and Schorfheide (2015), using a New Keynesian DSGE benchmark, showed systematic tension between model-implied low-inflation/deflation risk in several post-2008 periods and the central bank' s actual easing path—the macro-stabilizer function cannot be automatically aggregated from individual issuance discipline²³. When money contracts, the real value of debt burdens rises, potentially triggering a debt-deflation spiral and recession. Competing-currency theory has not supplied an adequate mechanism for this collective-action problem: individual issuers' supply discipline is individually rational; the collective consequence may be macro-level demand shortfall.

These two unresolved problems have new room for discussion in the blockchain-protocol era, but they have not disappeared. Protocol design must face them, not bypass them.

Network effects are the primary path of rebuttal: money' s value derives partly from general acceptance; first-mover advantage may yield winner-take-all rather than plural steady states. The engineering aim of interoperability standards (IBC, cross-chain bridges, VRC/ERC fungible interfaces) is to lower migration frictions so that holders can "vote with their feet" when rules deteriorate—yet the 2022 Terra/UST collapse showed that migration costs can be extremely high when liquidity dries up; as of 2024, Bitcoin still accounts for roughly half of crypto market capitalization, and USDT/USDC are highly concentrated among stablecoins²⁴—on-chain data do not yet confirm a stable plural competitive pattern. Cross-chain adjusted settlement-volume growth and non-head protocols' shares in vertical scenes (DeFi, gaming, supply chains) are observable positive indicators; head-protocol market-cap concentration, concentration at exchange and custody layers, and the fact that most retail still does not settle on-chain still conflict with the claim that "competition has dissolved monopoly."

On deflationary bias, elastic supply mechanisms offer another design path: Ethereum' s EIP-1559 introduced base-fee burn, so that supply contracts at peak network use (burn exceeds issuance) and expands at troughs (issuance exceeds burn), achieving automatic adjustment based on on-chain activity²⁵—demonstrating a technical possibility of introducing elasticity within a rule-constrained framework, far from a proven macro scheme superior to central banks' countercyclical tools; in a 2008-style deep recession, code rules as currently designed cannot actively play lender of last resort—a limit that must be understood alongside the welfare discussion of the 2 percent target under the New Keynesian framework in Chapter 3²⁶.

Section 10. From Banking Competition to Protocol Competition

The unit of competition is shifting from "notes issued by a bank, whose reputation attaches to institutional personality," toward "tokens and rules under a public protocol, whose reputation attaches to verifiable code and on-chain state." This shift touches a structural change in the basis of trust, far beyond mere terminological substitution—whether it has already occurred at the institutional level must be tested by observable indicators (fiat' s share in taxation and contracts; whether multi-rule monies obtain legal-tender or quasi-legal-tender status; adjusted on-chain payments as a share of global flows), not presupposed by a technology roadmap.

Historically, the trust chain of private bank money was: issuer reputation → dependence on disclosure and audit → dependence on auditors' independence → dependence on legal enforcement → ultimately dependence on state authority. The trust chain of on-chain protocol tokens by engineering design is: code rules → independently verifiable by anyone → rule changes require holder-community consensus → violations are automatically enforced on-chain (rather than depending on judicial process). On-chain tokens still require trust—but the locus of trust is designed to shift from personality to rules, from lagged accountability to ex ante verifiability; events such as FTX and Terra/UST in 2022 show that verifiability covers only constraints already on-chain and formalized—opaque reserves, governance capture, and breaches of off-chain promises can still break the chain.

What the public chooses, therefore, in theory is not only “which institution has better reputation,” but expands to: whether collateral mechanisms are transparent; whether governance prevents capture by a minority; whether interoperability keeps switching costs acceptable; whether compliance boundaries are compatible with mainstream legal environments; whether issuance rules are clear and hard to modify unilaterally. Each dimension is an open competitive dimension, and each under ideal conditions can be verified and thus priced by the market—real-world frictions include oracle feeds, thin-pool manipulation, MEV, and whale governance distorting “equal verifiability,” so that “protocol competition” at this stage remains closer to a disciplinary supplement in edge cases than a full substitute for central-bank discretionary macro stabilization.

The door Hayek opened lacked a suitable technical track in his time. Globally synchronized ledgers and verifiable rules allow the competitive unit to move from named bank monies toward verifiable protocol rule suites—in Chapter 9 of *The Denationalization of Money* he distinguished competition among named bank currencies, whereas homogeneous tokens issued in parallel by many parties leave no one responsible for the aggregate supply²⁷. Under floating exchange rates and on-chain liquidity markets, good-versus-bad comparison must be reunderstood. The dream of competing currencies is not obsolete; its form of realization must shift from competition of personality and reputation to competition of rules and protocols.

This evolution is closer to an extension of Hayek's thought than a negation. His most enduring contribution is a methodological stance: money should not be treated as a sacred public monopoly, but should, like other goods, submit to the test of competition; the dispersion of information requires decentralized mechanisms, not centralized discretion; good monetary institutions need embedded constraints, not reliance on issuers' virtue. In the blockchain-protocol era, these three positions are closer to feasibility at the technical layer than in Hayek's writing years—the institutional-layer transition remains long. When criticizing particular schemes, one must weigh valuable competitive logic separately from defective implementations; the empirical weight of on-chain experiments must still be placed on the same scale as free-banking historiography and the euro-area counterexample.

注释与引用

1. Hayek, 1976, *The Denationalization of Money*, p. 131: “Good money can come only from self-interest, not from benevolence.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
2. Hayek, 1978, “Competition as a Discovery Procedure,” in *New Studies in Philosophy, Politics, Economics and the History of Ideas*, University of Chicago Press, pp. 179–190: competition's function is to discover dispersed knowledge, not merely pursue static efficiency—aligned with ch04 §2's discussion of “the dream of competing currencies.” University of Chicago Press 1978 edition. ↩ ↩² ↩³

3. White, Lawrence H., *Free Banking in Britain* (Cambridge, 1984 1st ed.), ch. 2, pp. 40–52 (option clauses); ch. 4, pp. 76–95 (clearing networks); Selgin, George, “The Evolution of a Free Banking System,” *Economic Inquiry* 22(3), July 1984, pp. 289–300 (evolutionary model of competitive issue). ↩ ↩²
4. Selgin, George, *The Theory of Free Banking* (1988), ch. 2–4, pp. 25–78 (competitive issue, discount clearing, and supply discipline); Selgin & White, “How Would the Invisible Hand Handle Money?” *Journal of Economic Literature* 32(4), 1994, pp. 1718–1749. <https://doi.org/10.1257/jel.32.4.1718> ↩ ↩²
5. Calomiris, Charles W., “Deposit Insurance: Lessons from the Record.” *Economic Perspectives*, Federal Reserve Bank of Chicago, May/June 1989, pp. 2–41 (Scottish system and Bank of England lender-of-last-resort background); White, Lawrence H., “The Scottish Banking System before 1845: A Model for Laissez-Faire?” *Journal of Money, Credit and Banking* 27(2), 1995, pp. 421–431 (reply to institutional-background critiques). ↩ ↩²
6. Kroszner, Randall S., “Free Banking: The Scottish Experience as a Model for Emerging Economies?” *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31. https://files.stlouisfed.org/files/htdocs/publications/review/96/03/FreeBanking_Mar_Apr1996.pdf ↩
7. Weber, Warren E., “Resolving the Free Banking Debate,” *Federal Reserve Bank of Minneapolis Quarterly Review*, September 1994, pp. 2–8 (weights of Scottish vs. U.S. institutional variables; alongside Calomiris and Selgin narratives). <https://www.minneapolisfed.org/research/quarterly-review/resolving-the-free-banking-debate> ↩
8. Dowd, Kevin, *Laissez-Faire Banking*. Routledge, 1993, ch. 2–4 (competitive-issue models; clearinghouse-endogenized supply discipline); see also Dowd (ed.), *The Experience of Free Banking*, Routledge, 1992. ↩
9. Rockoff, Hugh, “The Free Banking Era: A Reexamination.” *Journal of Money, Credit and Banking* 6(2), 1974, pp. 141–167; see also Rockoff, “Lessons from the American Experience with Free Banking,” in Dowd (ed.), *The Experience of Free Banking* (1992), ch. 4. ↩ ↩² ↩³ ↩⁴
10. Selgin, George, “The Legal Restrictions Theory of Money: A Reappraisal.” *Cato Journal* 6(1), Spring/Summer 1986, pp. 479–497 (layered legal restrictions vs. competitive failure; read with Selgin 2010 on the 1865 federal tax and Calomiris & Haber 2014 on political bargains). <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1986/5/cj6n1-4.pdf> ↩
11. Selgin, George, “The Case for Free Banking: Then and Now.” *Cato Journal* 10(3), Winter 1991, pp. 539–552 (legal-restriction lists; transferable contemporary conditions; read with Selgin 1986/2010). <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1990/11/cj10n3-1.pdf>; White, Lawrence H., *Competition and Currency: Essays on Free Banking and Money*. New York University Press, 1989, ch. 1–3 (survey of free-banking theory), ch. 4 (Scottish option clauses); ch. 5–6 (internal school debate: fractional vs. 100% reserves). ↩ ↩²
12. Rockoff, Hugh, “The Free Banking Era: A Reexamination.” *Journal of Money, Credit and Banking* 6(2), 1974, pp. 141–167 (order of magnitude of note-issuing institutions and discount ranges around 1861); Spencer, “The Number of Banks in the United States, 1790–1860.” *Journal of Economic History* 25(3), 1965, pp. 421–428. ↩
13. Selgin, George, “The Suppression of State Banknotes: A Reconsideration.” *Economic Inquiry* 48(4), October 2010, pp. 931–942 (1865 10% federal tax, de facto parity, and exit of state banknotes). <https://doi.org/10.1111/j.1465-7295.2009.00260.x> ↩
14. Dwyer, Gerald P., “Wildcat Banking, Banking Panics, and Free Banking in the United States,” *Economic Inquiry* 34(4), October 1996, pp. 881–889 (wildcat geographic arbitrage and authentication costs); Timberlake, Richard H., “The Central Banking Role of Clearinghouse Associations,” *JMBC* 16(1), February 1984, pp. 1–15 (clearinghouse discount reflux). <https://doi.org/10.1111/j.1465-7295.1996.tb00123.x>; <https://doi.org/10.2307/1992521> ↩ ↩²
15. Hayek, 1976, *The Denationalization of Money*, p. 23: “impose upon existing monetary and financial agencies a very much needed discipline ... any deviations from the straight path of providing an honest money would at once lead to the rapid displacement of the offending currency by others.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
16. Hayek, 1976, *The Denationalization of Money*, ch. 22, “The Problem of Transition,” pp. 121–122 (transition requires granting competitive freedom at a stroke); revised edition preface (1978), p. 83, conceding the scheme may be “too radical.” Cross-ref. ch. 25 §1². PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
17. McKinsey & Artemis Analytics, “Stablecoins and the Future of Money” (2024); Visa Onchain Analytics adjusted metrics; see Chapter 1, Section 8, footnote ⁴, and Chapter 2, Section 7. ↩

18. Hayek, 1976, *The Denationalization of Money*, revised ed., ch. 1, "A Realistic Proposal" ("The Practical Proposal"): Common Market countries by treaty remove barriers to currency flows and cross-border banking, "preferable and more practicable than the utopian scheme of introducing a new European currency." Cross-ref. ch25 §1 ², §5. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
19. Eurostat, "Intra-EU trade in goods — main features" (intra-euro-area goods trade as share of intra-EU trade, rising in the 2000s); IMF COFER database, euro share of global allocated FX reserves peaking near 28% (around 2009). <https://www.imf.org/en/Statistics/COFER> ↩ ↩²
20. Mises, 1912, *The Theory of Money and Credit*, ch. 8 (regression theorem); Liberty Fund 1980 ed., pp. 111–123. <https://www.econlib.org/library/Mises/msT.html> ↩
21. Selgin, George, "Synthetic Commodity Money." *Journal of Financial Stability* 17, 2015, pp. 92–99. <https://doi.org/10.1016/j.jfs.2015.01.002> ↩
22. Mises, 1912, *The Theory of Money and Credit*, Liberty Fund 1980 ed., ch. 8, pp. 111–123 (regression theorem); see also Hayek, 1976, *The Denationalization of Money*, p. 43 on parallel currencies (*Parallelwährung*) and floating relative prices. <https://www.econlib.org/library/Mises/msT.html> ; PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
23. Del Negro, Marc P. Giannoni, and Frank Schorfheide. "Inflation in the Great Recession and New Keynesian Models." *American Economic Journal: Macroeconomics* 7(1), January 2015, pp. 168–196 (DSGE benchmarks for post-2008 inflation/deflation paths; contrast with collective deflationary bias under competitive issue). <https://doi.org/10.1257/mac.2013.029> ; cross-ref. ch03 §4 ⁹, ch09 §5 ²⁷. ↩
24. CoinGecko / Coin Metrics 2024 market-cap structure: Bitcoin roughly ~50% of total crypto market cap; USDT+USDC roughly ~80% of stablecoin market cap—concentration fluctuates with markets; order-of-magnitude reference, not a precise point-in-time snapshot. ↩
25. Ethereum Improvement Proposal 1559 (effective with the 2021 London upgrade): base-fee burn + tip incentives; supply elasticity depends on on-chain usage; intended to dampen extreme deflation/inflation swings; macro countercyclical efficacy has not been rigorously tested against traditional monetary policy. ↩
26. Woodford (2003), *Interest and Prices*, ch. 6 (pp. 235–280, welfare case for moderately positive inflation under nominal rigidities), ch. 7 (pp. 281–330, ELB and optimal average inflation); Galí (2015), *Monetary Policy, Inflation, and the Business Cycle*, 2nd ed., ch. 8 (pp. 145–180), ch. 15 (pp. 320–340, FIT). Sovereign NK 2% defense and boundaries of on-chain fixed rules / elastic supply: see Chapter 3, Section 4; Chapter 10, Section 8; Chapter 24, Section 2. ↩
27. Hayek, 1976, *The Denationalization of Money*, ch. 9, "Competition Between Banks Issuing Different Currencies," pp. 49–51: distinguishable named-currency competition; homogeneous tokens issued in parallel by many parties leave no one accountable for aggregate supply. Cross-ref. ch. 24 §5 ²⁷. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩ ↩² ↩³

§ 5 Good Money and Bad Money Revisited

For competing-currency theory to operate in practice, one must first clarify under what institutional premises “bad money drives out good” holds—and why, once legal parity is stripped away, the literature treats the Thiersian direction (good drives out bad) as a distinct mechanism rather than a simple “reversal” of the same law.

“Bad money drives out good” has become something of a shield, invoked against any monetary competition: as if, once multiple currencies coexist, the inferior must prevail, the superior withdraw, and ruin ensue. The phrase is cited far more often than it is carefully read. What Gresham observed was a particular phenomenon under particular institutional conditions; its core mechanism depends on a critical premise—legal parity, an official command fixing the exchange ratio between two monies while market valuations have already diverged from that ratio. Once that premise is removed, the direction of elimination is governed by market valuation and relative-price adjustment—what the literature calls Thiers’ Law, good driving out bad—but with this emphasis: it is another mechanism under different institutional premises, not an “inversion” of Gresham’s law under floating rates. One must first clarify Gresham’s precise meaning, its scope of application, and the trigger conditions for the Thiersian direction, before turning to elimination mechanisms under floating rates, on-chain liquidity, and standard-protocol environments—where the definitions of “good” and “bad” themselves are being rewritten by richer market signals.

Section 1. The Precise Context of Gresham’s Law

Thomas Gresham (1519–1579) was financial adviser to Queen Elizabeth I of England and founder of the Royal Exchange. In 1558 he wrote to the newly crowned queen describing the deterioration of English coinage: under Henry VIII the silver content of coins had been sharply reduced, and the poorer new coins circulated at one-to-one legal face value with older coins of higher silver content. Holders accordingly spent the inferior new coins first and hoarded or exported the superior old ones to the Continent—“bad money” drove “good money” from circulation.

The core mechanism of this observation is that legal parity creates arbitrage: when the official exchange ratio between two monies differs from market valuations, holders exploit the gap by spending the officially “overvalued” money (bad) and retaining the officially “undervalued” money (good). Bad money wins not because “bad” naturally conquers “good,” but because price controls create arbitrage opportunities; rational market behavior follows, and good money disappears from circulation.

This mechanism has recurred throughout history. In Ming–Qing China, copper cash and silver circulated in parallel under official exchange rates, yet market valuations shifted with supply and demand; when official ratios diverged from market valuations, the undervalued metal was hoarded or flowed abroad. During the nineteenth-century U.S. *Gold Acts*, official parity between gold and greenbacks was maintained while market spreads triggered systematic gold hoarding and export. In every case the trigger was official price control, not the essence of competition itself.

Correct application of Gresham’s law therefore requires checking two conditions: Is there a legal or officially enforced fixed exchange rate? Have market valuations of the two monies already diverged from that fixed ratio? Hayek stressed in *The Denationalization of Money*: “Gresham’s law will apply only to different kinds of money between which a fixed rate of exchange is enforced by Law”¹—only when both conditions are met does the prediction that “bad money drives out good” hold. Under freely floating rates there is no arbitrage opportunity to exploit; inferior money is reflected in market prices and voluntarily sold by holders.

Section 2. Thiers' Law: Another Direction of Elimination under Floating Relative Prices

Discussed alongside Gresham under floating relative prices and no forced parity is what is sometimes called "Thiers' Law," named for the French economist and statesman Adolphe Thiers (1797–1877); Rolnick and Weber (1986), using Minnesota free-banking-era data, contrasted it with the Gresham mechanism on institutional premises—when discounting is allowed the direction aligns with Thiers; when parity is forced, Gresham embeds². The logic is simple: when monetary relative prices can adjust with the market, money whose purchasing power continually depreciates is actively avoided by holders, relatively stable money is retained, and "good money" prevails in competition.

Historical cases give Thiers' Law broad support. Across decades of Argentine peso inflation, whenever official exchange controls loosened or were circumvented, dollars circulated in the market at a premium; during Venezuelan hyperinflation the bolívar was rapidly displaced by dollars and cryptocurrency. Zimbabwe's inflation peak, tax anchor, and "sanctity departed" mechanism are already detailed in Chapter 2, Section 5³—Hanke & Krus (2013), using official and black-market series, estimated the November 2008 monthly inflation peak at roughly 79.6 billion percent ($7.96 \times 10^{10}\%$); after dollarization in 2009 the domestic currency had functionally exited, while legal discontinuance came only in 2015—the C-money circle (tax nominal) and M-money circle (everyday store of value) can coexist in rift for years³. Here the emphasis is only on the Thiersian reading: bad money is actively abandoned, not Gresham arbitrage under legal parity; only when official and black-market rates diverge for long periods does superficially similar "spend local, keep dollars" behavior appear—one must not conflate similar directions with a "Gresham inversion." Charles Goodhart distinguishes "market money of account" (M-money, in the Mengerian saleableness tradition) from "state money of account" (C-money, in the Knapp–Innes tax-circle tradition): Zimbabwe and Argentina display a rift in which the C-money circle remains while M-money ranking has been rewritten—taxes still require domestic-currency nominal, yet everyday store of value and pricing have shifted to the dollar⁴. Thiers' Law describes M-money ranking; it does not automatically negate C-money's institutional floor. The tension between the two is key to understanding how "voting with one's feet" and "institutional chains still binding" can coexist.

In these cases legal status did not save inferior money; market behavior ultimately drove out the bad. Whether authentication costs can reproduce Gresham-like outcomes without parity still turns on information costs—legal parity alone does not uniquely determine the direction of elimination.

Free-banking historiography supplies finer-grained corroboration for the Thiersian direction. Analyzing competitive issue, Selgin noted that when banknotes circulate at market discount rather than legal parity, notes of overissuing banks are spent first and notes of prudent banks retained—consistent with Thiersian logic, except that "bad" and "good" are defined by clearing discounts rather than official exchange rates⁵. After the 1865 federal 10 percent tax on state banknotes, Selgin argued from issue statistics that state notes were forced to accept at parity and in practice exited circulation—legislation can rebuild *de facto* parity within a private system, blocking the Thiersian direction and re-embedding Gresham-style retention⁵. Selgin's 1986 "legal restrictions theory" generalizes the mechanism: it is not that "multiple issuers necessarily produce chaos," but that layered rules—parity laws, branching bans, holding taxes—determine whether relative prices can float—point-by-point comparable with Hayek's proposition at pp. 42–43 that "Gresham applies only under legal parity"⁶. Conversely, once legislation forces acceptance at face parity (or bans discounted circulation), the Gresham mechanism can re-embed in private banking: antebellum state "parity laws" for banknotes are, in Rockoff's and Selgin's historiographical reconstructions, precisely the institutional switch for bad notes remaining in circulation⁵. Rolnick and Weber, drawing on nineteenth-century Minnesota experience, further showed that so-called

“Gresham’s law” often fails statistically—the key remains whether forced parity exists; under free float, bad money discounts and good money premiums, in the Thiersian direction². Thus the good/bad direction depends not on “whether there are multiple issuers,” but on who fixes relative prices—Hayek’s distinction between Thiers and Gresham at pp. 42–43 of *The Denationalization of Money* and the empirical detail of free-banking literature can mutually corroborate.

A subtler manifestation occurs at the level of “soft substitution”: residents of high-inflation countries often do not conspicuously “dump the domestic currency,” but protect purchasing power through dispersed holdings—foreign-currency deposits where law permits, gold jewelry, real estate, or commodities. Such behavior may be invisible in macro statistics, yet it is a genuine signal of monetary holders voting with their feet. When central-bank foreign reserves come under pressure from such capital outflow, the response is often tighter capital controls—itself evidence that market pressure for “bad money driven out under free flow” is real.

Section 3. Cryptocurrency Competition under Floating Exchange Rates

Applying the Gresham–Thiers framework to contemporary cryptocurrency, the first finding is that token-to-token pairs in the crypto ecosystem almost never face legal parity—exchange rates among tokens are set in real time by automated market maker (AMM) protocols or centralized-exchange order books, without any institution fixing ratios. Hayek illustrated with the end of Weimar inflation: when exchange rates float freely, “people refuse to accept inferior money and insist on superior money”⁷—the price-control-driven circulation of bad money scarcely exists between pure floating pairs; crypto-asset competition is closer to the Thiersian framework in relative-price mechanism.

Stablecoins do see adoption in cross-border corridors and high-inflation edge cases, yet on-chain real payments remain marginal in global payment flows (three metrics and data in Chapter 1, Section 8)⁸—the Thiersian direction is observable within crypto submarkets but cannot yet be extrapolated as displacement of fiat monopoly. Moreover, dollar-pegged stablecoins (USDT/USDC) functionally play a “1:1 parity” role: issuers promise redemption, and regulation and audit constrain deviation—this is not the same institution as Hayekian “pure floating competition after abolishing forced legal tender”; algorithmic Terra/UST’s 1:1 peg depended on sentiment and mint–burn mechanisms and failed rapidly in confidence crises—showing that parity need not appear as legal compulsion, yet can still produce Gresham-like retention and death spirals, with the trigger shifting from legal command to protocol promise and market belief.

For the Thiersian direction to hold, two testable premises must also be met: relative prices can adjust with the market, and quality signals can be verified at low cost. On-chain rule transparency favors the second, yet oracle price feeds, thin-pool manipulation, cross-chain bridge custody, and exchange concentration can still raise verification costs, allowing short-run “bad” assets to linger in circulation via liquidity subsidies or narrative premiums—surface outcomes sometimes resemble Gresham, yet the mechanism is information lag and incentive distortion, not legal-parity arbitrage.

Under this framework, holders’ choice criteria expand beyond the single dimension of “purchasing-power stability” in traditional monetary analysis to multidimensional evaluation. A token’s degree of “goodness” is priced by the market across several dimensions.

Transparency and credibility of issuance rules come first: Is the supply cap clear and verifiable? Do historical issuance records match white-paper commitments? Can governance resist “governance attacks” that alter critical parameters? Bitcoin supporters prize this dimension highly, treating the 21-million-coin cap as core value; holders of other tokens accept more flexible monetary policy in exchange for functional extensibility.

Liquidity depth and market acceptance follow closely: Can one buy and sell on major exchanges at reasonable slippage? Is the token accepted as collateral by mainstream DeFi lending protocols? If a token cannot flow smoothly into major financial Lego components, its usefulness as money or store of value is limited, and market valuation will reflect that constraint.

Depth of ecological application measures what developers build upon it—both a technical metric and a proxy for economic usefulness: the deeper the ecosystem, the more scenes in which the token has real demand; “demand-driven liquidity” is more robust than “incentive-driven liquidity.”

Section 4. Liquidity: The Modern Version of the Gresham Test

Liquidity depth is the most direct “good/bad” judgment test in on-chain environments. Automated market makers (AMMs) externalize liquidity in mathematical formulas: a token pool’s reserves directly determine the price impact of a given trade size. This information is real-time inspectable by anyone—transparency traditional money markets cannot match.

Yet “liquidity” can be driven by real demand or artificially stacked by incentives. The most common form of on-chain liquidity manipulation is “liquidity mining”: projects attract liquidity providers with high token rewards, manufacturing superficially deep pools. Capital floods in when reward rates are high and exits rapidly when they fall—leaving ruins of liquidity collapse and sharp price drops. Early injectors who cash out at high prices profit; later holders bear losses. This is not bad money driving out good in the Gresham sense (there is no legal pricing arbitrage on-chain), but short-run signal distortion manufactured by artificial incentive gradients, systematically transferring gains from later entrants after capital is attracted.

Distinguishing real from artificial liquidity requires comparing several metrics: liquidity relative to total market cap (may be anomalously high under heavy incentives, collapsing after incentives exit); average holding time of liquidity providers (long-term holders withstand premature exit better than reward chasers); historical stability of pools (liquidity that survives different market conditions is more real). Analyzing free-banking “face-parity laws,” Selgin noted that once legislation bans discounting or forces face acceptance, inferior notes linger in circulation—on-chain liquidity mining’s high-yield subsidies are structurally isomorphic: short-run incentives manufacture de facto parity acceptance; when subsidies ebb, inferior projects’ liquidity collapses⁹. The full mechanism of incentive distortion and tokenomics design problems. Over recent cycles the crypto ecosystem has accumulated market intuition for distinguishing the two, but the learning process is costly—DeFi total value locked (TVL) jumped from roughly \$1 billion early in 2020 to a peak above \$180 billion, then fell below about \$500 billion after incentives ebbed in 2022¹⁰; “costly” here has concrete magnitude: large numbers of late, information-asymmetric participants bore the main losses.

Section 5. Bubble Cycles and the Market’s Self-Cleaning Logic

On-chain good/bad competition also exhibits a self-reinforcing cyclical distortion. In high-sentiment periods, new projects’ token reward rates are high enough to attract large liquidity inflows and push prices up; rising prices generate “wealth effects,” attracting more new participants and further lifting prices—a classic positive-feedback structure. In that process, “good” projects with real demand support and “bad” ones that pile up false demand purely via incentives are hard to distinguish on surface numbers, because both prices rise and both display the illusion of “ample liquidity.” This differs from Gresham’s law, which requires legal-parity premises¹; here market sentiment and incentive gradients distort quality signals, postponing good/bad discrimination until after the bubble bursts.

The order of bubble collapse usually runs inverse to the strength of “real demand”: projects lacking real use cases lose liquidity first and prices go to zero; projects with partial real demand but poorly designed incentives suffer sharp drawdowns; only a few protocols with real use cases, robust incentive design, and strong ecosystems maintain meaningful market caps and liquidity after the cycle turns down. In 2018 total crypto market cap fell from a peak near \$800 billion to about \$130 billion; in 2022 from a peak near \$3 trillion to about \$800 billion¹¹—both major bear-market cleansings roughly followed that order, though each cleansing also hit some “good” projects indiscriminately via liquidity crises, imperfectly achieving “bad cleared, good continued.” Market self-cleaning is a directional proposition, not an instantaneous justice mechanism.

The market’s self-cleaning function does exist, but its operating cost is high: large numbers of late, information-asymmetric participants (mainly retail) bear the main losses, while early “prescient” large holders have often already exited at highs. This distributional asymmetry is not unique to blockchain; any speculative new asset class undergoes similar price-discovery pain in maturation—the internet bubble and railway mania both left marks of excess and liquidation. Recognizing the cycle requires a long-term view of on-chain good/bad competition: competition is an effective screening mechanism, yet in the short to medium run sentiment and incentives can sharply distort screening clarity and fairness.

Section 6. Standard Interfaces: Infrastructure for Good/Bad Competition

In Gresham’s era, switching from one money to another required finding exchangers, paying discounts, and bearing authentication risk; switching costs systematically affected which money was used, even allowing inferior money to remain in circulation because of those costs. Today blockchain standard interfaces compress switching costs to the technical-adaptation layer.

ERC-20—the technical standard for tokens on Ethereum—defines the minimal interface set a token must implement: `transfer`, `approve`, `allowance`, `balanceOf`, `totalSupply`. Any token following this standard automatically works with all ERC-20-supporting wallets, exchange interfaces, block explorers, and DeFi protocols. That means the technical time from deploying a new token to wallet display and DEX trading can be hours—not the months of compliance required to open a new account type in traditional finance.

Standards lower switching costs, but standards themselves are objects of competition. Token standards on different chains (Ethereum’s ERC-20, TRON’s TRC-20, Openverse’s VRC-20, and so on) share similar design ideas but differ in detail; without interoperability across chains, liquidity islands form, users must maintain different accounts on different chains, and cross-holding frictions remain. Per the Openverse white paper, VRC-20 provides within a given network a minimal interface similar to ERC-20 (`transfer`, `balanceOf`, `approve`, etc.) so wallets and DApps can compose calls—whether that path can achieve ERC-20-scale adoption and audit depth in mainstream ecosystems awaits mainnet and cross-chain interoperability practice, and should not be extrapolated from roadmaps as accomplished fact.

From the perspective of good/bad competition, the significance of standards is this: they make “good” easier to identify and adopt, and “bad” easier to detect and discard. When switching costs are extremely low, markets respond faster to monetary quality, and the cost to issuers of maintaining inferior rules rises sharply. White (1994) stressed that what competitive issue most struggles to close is often unit-of-account convergence—when multiple private monies coexist, which sets the price list?—the same class of problem as ERC-20/VRC-20 lowering switching costs without necessarily solving the unit-of-account issue⁹. This is one technical realization path for the competitive mechanism Hayek envisioned—premised on abolishing forced legal tender and allowing monies to compete freely at market exchange rates¹².

Section 7. Good and Bad under Functional Stratification

Traditional monetary analysis defines “good” as purchasing-power stability, reasonable in a fiat background centered on store of value and everyday unit of account. Yet the crypto ecosystem has functional stratification: different asset types serve different purposes and correspond to different standards of “good.”

“Good” for stablecoins: degree of deviation from the peg target (usually the dollar), adequacy of collateral, depth of liquidity, regulatory compliance status. The May 2022 collapse of algorithmic TerraUSD (UST) remains one of the largest stablecoin failures to date. Its design depended on a mint–burn mechanism with LUNA to maintain the peg, without exogenous hard-asset reserves; when market confidence cracked, selling pressure triggered a UST–LUNA death spiral, and both approached zero in under two weeks, evaporating peak combined market value on the order of \$40 billion¹³. This is functional “bad”—a stablecoin’s core function is stability, and UST thoroughly destabilized under stress; the peg mechanism became a feedback loop amplifying collapse rather than a buffer. Post-mortems attribute failure to a combination of reflexive pegs, thin-pool liquidity, and misaligned governance incentives, not a single parameter error¹³.

By contrast, MakerDAO’s DAI is overcollateralized with on-chain assets, with liquidation written into smart contracts and triggered automatically when the collateral ratio falls below a threshold. On 12 March 2020 (“Black Thursday”), ETH plunged roughly 30%, triggering mass liquidations and DAI premiums into roughly the \$1.06–1.12 range; Maker community post-mortems recorded zero-price auctions and emergency governance parameter adjustments¹⁴. Under extreme stress DAI roughly held the peg, but deviation and repair costs show that the overcollateralized path is more robust, not frictionlessly immune—“good” is the result of relative comparison and institutional learning, not an absolute guarantee.

“Good” for governance tokens: fee income actually generated by the protocol and the share accruing to token holders; whether governance weight prevents concentrated control; real ecological activity (not incentive-driven).

“Good” for store-of-value assets: credibility of scarcity commitments; censorship resistance; degree of network decentralization. Bitcoin supporters prize these three, especially the second and third—because traditional assets (gold, fiat deposits) can be seized or confiscated, and Bitcoin’s censorship resistance under self-custody is a distinctive advantage.

The implication of functional stratification is that good/bad competition does not occur on a single axis but unfolds simultaneously across multiple dimensions. Comparisons across asset types are apples-to-oranges; the definition of “good” must first specify the object of evaluation and the use case.

Section 8. The Philosophy of Algorithmic Stability: Limits of Pure Rules and Hybrid Paths

After the stablecoin crisis, the crypto ecosystem reached a relatively mature consensus: pure algorithmic stability (no exogenous collateral, fully dependent on arbitrage mechanisms and dual-token structures), without sufficient external demand support, readily falls into death spirals under confidence crises. This case of “pure-rule failure” puts an expensive question mark beside the view that “if rules are clever enough, collateral is unnecessary.”

Yet the core disagreement concerns what rules can and cannot substitute. Rules can precisely define execution logic under specified conditions, but robustness depends on whether those “specified conditions” cover extremes. TerraUSD’s fatal flaw was that its arbitrage mechanism assumed always-present LUNA demand—itsself sentimental and able to vanish suddenly; when sentiment reversed, the rules executed correctly, but in the direction of accelerating collapse. The deep problem of rule design is how external assumptions fail under extreme conditions.

The robustness of overcollateralized paths (such as DAI) comes from independence of reserve value: even under extreme pessimism, so long as collateral value (usually ETH or other mainstream assets) holds above some level, liquidation still protects holders. This is a hybrid of “rules + external anchor”: rules supply execution certainty; the external anchor supplies an independent value base. Neither is dispensable—rules without independent collateral leave the system fragile to external shocks; collateral without rules leaves execution dependent on human intervention and loses the value of decentralization.

Fiat-backed stablecoins (such as USDC) push the hybrid to an extreme: their “rule” is that the issuer holds dollar reserves and accepts audit; stability comes from traditional-finance credit backing. This is not the purest “trustlessness” at the on-chain technical layer, but it is the most stable at the user-experience layer. Three paths coexist in the market, serving holders with different needs—precisely the multidimensional definition of “good” in practice.

Section 9. Network Effects and Benign Lock-In

Outcomes of good/bad competition are shaped not only by quality but jointly by first-mover advantage and network effects. Money’s value partly derives from wide acceptability, which rises with the number of users—a classic network-effect structure. In markets with strong network effects, winner-take-all is a common output, not pluralistic steady states.

Bitcoin’s “digital gold” positioning has faced multiple “technically superior challengers” over more than a decade, yet as of 2024 still held roughly 50%–55% of total crypto market cap¹⁵. Ethereum’s smart-contract platform status, amid recurring “ETH killer” narratives, has long accounted for over 60% of DeFi locked value across the ecosystem¹⁰. Both have known technical limits yet still maintain dominance—network effects self-reinforce: more users → more liquidity → more developers → more applications → more users. This concentration aligns with the concern in Chapter 4, Section 9, “scale effects and new monopolies”: Thiersian victory of good money does not automatically equal pluralistic steady states.

Network effects can “lock in benign standards” or “lock in inferior equilibria.” If first-mover advantage happens to belong to a superior design, network effects help: they accelerate adoption of good money and raise high barriers for later inferior substitutes. If first-mover advantage happens to belong to an inferior design, network effects delay upgrade—as with the QWERTY keyboard, technically superior alternatives exist, but switching and coordination costs keep the existing standard stable. In money the problem is especially sharp, because monetary network effects are far stronger than keyboard layouts and coordination costs of switching are higher.

There is no universal answer to this tension, but there is a concrete design implication: if superior standards are to displace suboptimal ones, switching costs must be acceptable and transitional bridges must exist between new and old standards—one cannot expect all users to switch synchronously. Protocol interoperability, cross-chain bridges, and multi-chain wallets are technical means of lowering network-effect lock-in costs.

Section 10. Regulatory Arbitrage and Exogenous Constraints on Good/Bad Competition

Good/bad competition occurs not only inside markets but is deeply shaped by regulatory frameworks. Differing jurisdictional attitudes toward crypto assets create regulatory-arbitrage space, and that space itself affects competitive outcomes. If a well-designed protocol cannot gain institutional adoption in major markets because of regulatory uncertainty, while a weaker competitor operating freely in a lax environment gains liquidity, the regulatory framework distorts market-screening signals.

SEC enforcement actions against multiple crypto projects in 2022–2023 deemed some tokens unregistered securities¹⁶. That determination depends not on technical design or economic-mechanism quality, but on the Howey Test—whether there is investment of money, a common enterprise, and expectation of profits from others’ efforts. A carefully designed decentralized token under protocol standards may be deemed a security because of early token-allocation methods; a weaker economic mechanism that successfully decentralizes may evade securities-law application. Legal screening and market screening may therefore point different ways—the regulatory framework itself is an exogenous variable in good/bad competition; one cannot assume on-chain Thiersian mechanisms operate in a vacuum.

There is no simple solution to this contradiction, but there is an institutional exit: clear legal frameworks can reduce competitive distortion from uncertainty. The EU Markets in Crypto-Assets Regulation (MiCA), phased in from 2024, sets unified disclosure and reserve requirements for stablecoins and CASPs (crypto-asset service providers)¹⁷—practitioners treat it as a case of “rule clarity,” even where some clauses are stricter. The more predictable the rules, the less market screening is distorted by regulatory arbitrage alone; whether MiCA in practice lowers distortion still awaits enforcement and cross-border coordination tests, and should not be presumed a sufficient condition for competitive discipline.

Section 11. Design Problems of Competition in the Protocol Era

Discussion of good and bad money in the protocol era reduces to several interlocking design choices: how issuance rules trade off transparency and revisability; how liquidity incentives reflect real demand rather than short-run arbitrage; how standard interfaces compress switching costs low enough; how network effects avoid freezing first-mover advantage into permanent monopoly. These problems have no general answers detached from concrete protocols. Competition is no longer only a philosophical proposition but a daily on-chain contest of liquidity, adoption, and code quality—every contract call, every new protocol adopted, is a real-time market vote on the good/bad question.

Gresham’s history tells us that even when competition exists, the wrong institutional framework produces distorted outputs of “bad winning, good losing.” The on-chain ecosystem continues to evolve in incentive design, governance structure, and standardization; formation of the “right institutional framework” is a learning process requiring repeated market validation and rule iteration. That process cannot be shortened, but it can be learned consciously—each failure case is an information output about “what rules are infeasible,” valuable though costly.

From Gresham to Thiers, from Scottish free banking to the TerraUSD collapse, the story of good/bad competition spans five centuries; technical forms change while incentive logic does not. The pursuit of “good” is real; vigilance toward institutional conditions that give “bad” short-run advantage must not relax.

When full information, low switching costs, and enforceable rules are in place, good money tends to accumulate advantage, while bad money faces continuing liquidity pressure and user attrition. But these three conditions must be actively built and maintained; they are not public goods the market automatically produces—the responsibility of protocol designers is to construct information and incentive environments that let markets distinguish good from bad effectively¹⁸. Between “relative prices can float” and “bad money is driven out” lie three further thresholds: liquidity depth, verification cost, and compliant accessibility; on-chain experiments provide observation windows, yet the core position of global retail and sovereign monetary institutions has not switched.

Competition itself is a means; the end is to discover and promote better monetary institutional arrangements: competition under price controls drives out good money; competition under free float drives out bad; the on-chain ecosystem’s “institutional framework” includes technical standards, incentive design, and governance structure

—not only legal provisions. Overestimating the automaticity of Thiers’ Law and underestimating the marginal contribution of rule verifiability to discipline equally distort judgment—the prudent conclusion is: direction can be argued; timing cannot be prophesied.

注释与引用

1. Hayek, 1976, *The Denationalization of Money*, p. 42: “Gresham’s law will apply only to different kinds of money between which a fixed rate of exchange is enforced by Law.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↗ ↗²
2. Rolnick, Arthur J., and Warren E. Weber, “Gresham’s Law or Gresham’s Fallacy?” *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1986, pp. 17–30. <https://www.minneapolisfed.org/research/quarterly-review/greshams-law-or-gresham-s-fallacy> ↗ ↗²
3. Chapter 2, Section 5 (Zimbabwe: tax anchor, Hanke hyperinflation peak, 2009 dollarization and 2015 formal discontinuance); Chapter 7, Section 1 (Goodhart M/C-money juxtaposition), Section 7 (Hayek Gresham/Thiers boundary). Hanke, S. H. & Krus, N. (2013), “World Hyperinflations,” *Cato Working Paper* (November 2008 monthly inflation peak ~79.6 billion %); Hanke, Zimbabwe Hyperinflation Index. <https://www.cato.org/research/working-papers/world-hyperinflations> ↗ ↗²
4. Goodhart, Charles A. E., “The two concepts of money: implications for the analysis of optimal currency areas.” *Economic Journal* 108(447), 1998, pp. 377–390 (M-money and C-money; tax circle vs. market saleableness ranking). <https://doi.org/10.1111/1468-0297.00291> ↗
5. Selgin, George, *The Theory of Free Banking* (1988), ch. 3 (discount clearing and “good notes retained”); Selgin, “The Suppression of State Banknotes: A Reconsideration,” *Economic Inquiry* 48(4), 2010, pp. 931–942 (1865 federal tax and de facto parity); Rockoff, Hugh, “The Free Banking Era: A Reexamination,” *Journal of Money, Credit and Banking* 6(2), 1974, pp. 141–167. <https://doi.org/10.2307/1990856> ↗ ↗² ↗³
6. Selgin, George, “The Legal Restrictions Theory of Money: A Reappraisal.” *Cato Journal* 6(1), Spring/Summer 1986, pp. 479–497 (1865 holding tax, parity laws, and branching restrictions as institutional switches for Thiers/Gresham direction); cross-ref. Chapter 4, Section 2 [^24], Chapter 7, Section 6. <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1986/5/cj6n1-4.pdf> ↗
7. Hayek, 1976, *The Denationalization of Money*, p. 43: at the end of Weimar hyperinflation, after fixed rates failed, “good money drives out bad”—holders refuse inferior money and demand superior. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↗
8. McKinsey Global Payments Report 2024; Artemis Analytics stablecoin payment volume estimates (~\$390 billion/year order of magnitude); cross-ref. Chapter 1, Section 8, Chapter 4, Section 9. Global payments ~\$200 trillion/year order of magnitude; on-chain share ~0.02% is a directional estimate varying with the definition of “adjusted real payments.” ↗
9. Selgin, George, *The Theory of Free Banking* (1988), ch. 3, pp. 45–58 (face-parity laws and discount clearing; structural contrast with liquidity-mining incentive distortion); White, Lawrence H., “Competitive Payments Systems and the Unit of Account,” *AER* 84(3), June 1994, pp. 699–712 (competitive issue and unit-of-account convergence). <https://doi.org/10.1257/aer.84.3.699> ↗ ↗²
10. DeFi Llama TVL historical series: early 2020 ~\$1 billion → November 2021 peak above \$180 billion → end-2022 below ~\$50 billion; Ethereum DeFi TVL long ~60%–70% of ecosystem. <https://defillama.com/> ↗ ↗²
11. CoinGecko Global Market Cap Chart: January 2018 peak ~\$830 billion → December 2018 ~\$130 billion; November 2021 peak ~\$3.0 trillion → December 2022 ~\$830 billion. <https://www.coingecko.com/en/global-charts> ↗
12. Hayek, 1976, *The Denationalization of Money*, pp. 23, 42: the competitive scheme requires “depriving government … of the power of making any money ‘legal tender’” for market discipline to take effect. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↗

13. Terra/UST collapse: 7–13 May 2022 UST depeg and LUNA death spiral; peak combined market value ~\$40 billion order of magnitude (CoinGecko/CoinMarketCap historical data). Post-analysis: BIS Working Papers No. 1075, "Stablecoins and crypto assets: lessons from the Terra/Luna crash" (2023); IMF *Global Financial Stability Report* Oct 2022, ch. 2. ↩ ↩²
14. MakerDAO community, 12 March 2020 "Black Thursday Post Mortem": ETH crash triggering liquidation spiral, zero-price auctions, and DAI premium; Forum: <https://forum.makerdao.com/> . DAI premium range from on-chain oracles and Dune Analytics historical series. ↩
15. CoinGecko / Coin Metrics, 2024 Bitcoin market cap ~50%–55% of total crypto (varies with cycles). Cross-ref. Chapter 4, Section 9 head-concentration discussion. ↩
16. SEC v. Ripple Labs (2023), SEC 2023 enforcement and Wells Notice series against Coinbase, Binance, et al.; Howey Test in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). ↩
17. Regulation (EU) 2023/1114 (MiCA), phased application to stablecoin issuers and CASPs from 30 June 2024; official text of the European Parliament and Council: <https://eur-lex.europa.eu/> ↩
18. Kroszner, Randall S., "Free Banking: The Scottish Experience as a Model for Emerging Economies?" *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31 (extrapolation must distinguish community scale, clearing infrastructure, and legal enforcement); White, Lawrence H., "Competitive Payments Systems and the Unit of Account," *American Economic Review* 84(3), June 1994, pp. 699–712 (unit of account and switching costs in competitive payment systems). ↩

§ 6 Global Ledger and Verifiable Rules

Good/bad competition depends on verifiable information and low-cost switching; the global ledger and programmable rules supply the technical base for those conditions.

Every major turn in monetary history has accompanied an upgrade in recording and verification technology. From verifying weight and fineness of commodity money, to mint marks on metallic coin, to anti-counterfeit printing of paper notes, to double-entry bookkeeping in commercial banks, to electronic archives in central clearing systems—each recording technology defined a form of trust: whose ledger counts, who may amend, who may contest. In October 2008 a nine-page white paper proposed a new recording technology: without a central institution, anyone could join the network, verify the ledger, and participate in bookkeeping, all independent of any particular trust relationship. What it rewrote was far more than payment efficiency; it was the infrastructure on which trust itself is built. The foundational leap from Bitcoin to smart-contract platforms rewrote both the meaning of “verifiable rules” and the rules of the monetary-competition game—fiat would not vanish, but “rules over persons” for the first time acquired an engineerable technical path in global monetary competition.

Section 1. What Satoshi Changed

Bitcoin applied for no banking license and lobbied no legislature. Its inventor was an anonymous or pseudonymous individual (or group) using the name “Satoshi Nakamoto,” who submitted a white paper to a cryptography mailing list in the shadow of the 2008 financial crisis and, on 3 January 2009, launched the first block—the genesis block. Embedded in the genesis block’s coinbase transaction was a line of text: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” That line is a timestamp and a manifesto: a monetary system that needs no bailout and depends on no chancellor was starting.

Bitcoin’s architecture reflects a systematic critique of existing monetary institutions. Byzantine-fault-tolerant consensus solved the engineering problem of “reaching state agreement in a network of untrusted participants”; proof of work (PoW) made ledger tampering costlier than its benefit (rewriting history requires more than 50% of hash power)—Satoshi’s white paper §4 explicitly traces PoW to Adam Back’s Hashcash anti-spam mechanism, embedding “verifiable computational cost” in issuance discipline¹; the white paper’s references also credit Wei Dai’s b-money proposal (1998)—a precursor chain of distributed ledgers and proof of work²; Szabo’s 2005 “bit gold” and 1998 “Secure Property Titles” had already sketched distributed property registration and timestamp chains, and Hal Finney’s 2004 RPOW (Reusable Proofs of Work) was the engineering middle link between Szabo’s vision and Satoshi’s chained ledger³; issuance rules were written into genesis code, halving every 210,000 blocks, with a hard cap of 21 million coins. Changing any of these core parameters requires broad consensus among network nodes and miners—in practice equivalent to the birth of a new money, not an “upgrade” of the old.

The precise description of the core innovation is: do not trust the issuer’s person; verify whether rules are obeyed. When Hayek envisioned circulation of private tokens, he described a paper-money system that global institutions could “freely issue and compete,” with issuers sustaining themselves by purchasing-power stability⁴—structurally different from metallic-era reliance on physical attributes (coin fineness) and paper-era reliance on institutional promises (central-bank backing). Holders can run a full node themselves, independently verify current ledger state and historical issuance, without any intermediary telling them the truth. This moves the foundation of monetary trust from “believe an institution’s promise” to “verify the logic of mathematics and code.” The former can be altered by political pressure; the latter cannot.

Yet Bitcoin's design also contains limits. Base-layer throughput of roughly seven transactions per second cannot directly serve global retail payments; energy consumption remains contested; lack of programmability limits direct use in complex financial logic. Satoshi solved "how to build a value ledger without a trusted third party"—a foundational, most important problem; but the full functions of money and finance far exceed a "trusted ledger," which is what post-Bitcoin protocol exploration must answer.

Section 2. Ethereum: Embedding Money in a Programmable Environment

In 2013, nineteen-year-old Vitalik Buterin released the Ethereum white paper with a question: if the blockchain were not only a monetary ledger but a Turing-complete execution environment, and "state" were not only balances but arbitrary program state, what would happen? "Smart contracts" were not Buterin's invention—cryptography pioneer Nick Szabo had proposed the idea in the 1990s⁵—but Buterin first combined them with the immutability of blockchain ledgers and offered a concrete path to a "programmable blockchain"; Gavin Wood's Yellow Paper §§1–2 formalizes Ethereum as a state-transition system, and §4.2 meters execution cost with Gas, making "deploy equals issue" technically auditable⁵.

When Ethereum mainnet launched in 2015, embedding "money" in a programmable environment opened a door Bitcoin had not. Projects could deploy token contracts in days, defining supply, transfer rules, approval logic, mint and burn conditions—all written as open-source code, deployed to an immutable chain, readable by anyone to verify that rules match claims. This turned "transparent issuance rules" from verbal promise into a fact independently checkable in technology.

The 2017 ICO (initial coin offering) wave was rare in both scale and chaos. Per CoinSchedule and Fabric Ventures summaries, 2017 token sales raised about \$5.6 billion across more than a thousand projects, a substantial share later judged fraudulent or lacking deliverable products⁶—an early lesson that possibility (anyone can issue) is not reality (sustainable money). Yet the chaos had a constructive side: it was humanity's first large-scale public test of combining "standardized issuance interfaces" with "market self-screening." The ERC-20 standard made any token technically immediately tradable; the market—not regulators—became the first filter: projects with real demand and development progress accumulated liquidity and users; hollow projects saw liquidity dry up after the valuation bubble burst, and prices went to zero. The process was brutal, but the lessons were encoded into subsequent protocol design norms and market evaluation frameworks.

Section 3. Composability: Money as the Base of Financial Lego

Ethereum's most distinctive innovation is the emergent architectural property of "composability," not any single protocol. Within the same address space, any address holding an ERC-20 token can interact with every protocol designed to accept that token—no new account, no approval, no bilateral negotiation. One approval transaction and one call transaction suffice to deposit a token into a lending protocol, liquidity pool, or derivatives position.

This expands monetary competition from "which banknote to choose" to "which set of financial Lego to choose." In traditional finance, commercial-bank accounts, securities custody, FX accounts, and trust accounts belong to different institutions, regulatory frameworks, and settlement cycles; interoperability depends on complex compliance agreements and correspondent arrangements. An on-chain account can complete multi-step operations in a single transaction: swap ETH for stablecoins, deposit stablecoins in a lending protocol for interest, compound interest into another yield strategy—without human intervention, counterparty confirmation, or third-party custody. That is a marked rise in financial-infrastructure efficiency, enabled by ledger unity (all

assets on one chain’ s state machine) and contract interoperability (any contract can call any contract whose interface is public).

Composability’ s risk is a structural upgrade of “contagion risk.” In traditional finance, inter-institutional dependence is complex but mostly bounded by compliance and isolation (segregated margin, custody versus proprietary). On-chain, call graphs can nest to arbitrary depth; losses from one protocol bug can propagate along dependency chains. In March 2023 Euler Finance suffered a flash-loan attack; even on-chain-verifiable collateral logic failed to prevent roughly \$197 million in losses⁷; the same year’ s Mango Markets and Curve incidents showed that oracle manipulation can trigger cross-protocol liquidation cascades—verifiable execution does not automatically equal true inputs. Isolation is not the answer, but security standardization and risk-isolation design must become routine discipline in protocol development.

Section 4. Verifiable Rules: Execution, State, and History

“Verifiable rules,” as the core promise of blockchain monetary systems, must be decomposed into concrete technical layers before advantages and limits can be seen clearly.

Layer one: verifiable execution. Once rules are written into a smart contract and deployed, they execute automatically without depending on the deployer’ s later actions. A typical CDP (such as MakerDAO/DAI) automatically triggers forced auction when the collateral ratio falls below liquidation line L , without waiting for the issuer to “decide” whether to liquidate—VRC-10/PCIM and VRC-11 native rules set no L/W ; extreme-market stress paths are redemption runs and reserve depletion (public domain) or off-chain payout runs (private domain); tokens unlock automatically when lockup expires, without holder application; when a governance proposal reaches quorum, parameters update automatically without manual admin execution. This layer’ s credibility is strongest because it turns rule execution from “promise” into “determinism”—so long as contract code is correct, outcomes can be predicted in advance by anyone.

Layer two: verifiable state. The blockchain ledger’ s current state is real-time inspectable by anyone running a full node: who holds what, balances, current contract parameters (collateral ratios, fees, locked amounts). This turns asset verification from “depend on institutional statements” into “independently queryable.” Audit shifts from periodic professional activity to anytime operation by anyone with technical capacity. In traditional finance investors rely on quarterly fund NAV disclosure; on-chain, anyone can query a protocol’ s true state in real time, with no informational advantage from time lag.

Layer three: verifiable history. All historical transactions and contract calls are permanently recorded on-chain, traceable, auditable, and undeletable—at least not by a single party, unless controlling more than 50% of hash power or stake (depending on consensus). This supplies the most complete public transaction archive yet for regulatory compliance, dispute resolution, and historical research. Traditional finance’ s historical data are partly private and partly fragmented; on-chain history is a public good; anyone can independently verify ledger state at a past point in time.

The three layers of verifiability jointly constitute the technical foundation of the promise “rules over persons.” Mises stressed in *Human Action* that without calculable price signals, rational economic planning is impossible; on-chain verifiable rules make monetary issuance parameters public information anyone can independently check, partly answering the Austrian school’ s twin concerns of “dispersed knowledge” and “calculability”⁸.

In §§1–2 of his 1892 *On the Origin of Money*, Menger defined “saleableness” as the ease of resale market participants accept to complete exchange: ranking rests on breadth of demand, divisibility, durability, and portability, not prior state endorsement⁹. Kiyotaki and Wright formalized the same intuition in search-theoretic

monetary models: in a random-matching bilateral search economy, holding assets “easier to exchange for desired goods in the next trade” strictly dominates holding low-saleableness assets—money thus emerges as the equilibrium object that minimizes search frictions, without central coordination¹⁰. Kiyotaki & Wright (1993) *AER* further distinguish intrinsic saleableness (the good’s own uses) from extrinsic saleableness (belief in wide acceptance as medium), showing that even assets without industrial use can be monetary equilibria if enough participants expect others to accept them—supplying a computable contrast framework between Menger’s “attribute ranking drives emergence” and Mises’ s “must trace back to commodity demand”: the former stresses equilibrium selection dynamics; the latter stresses hermeneutic constraints of historical price chains¹⁰. Szabo in “Shelling Out” (2002) supplements the same emergence logic from prehistoric collectibles cooperation; in “Money, Blockchains, and Social Scalability” (2017) he defines social scalability as: when participants need not know one another to collaborate, verifiable rules substitute for interpersonal trust costs—aligned with the second dimension of “verifiability” below¹¹. He wrote that people “Bringen ... die wirtschaftlichsten Güter ... an die Stelle des unmittelbaren Tausches”—pushing the economically most easily disposed goods into indirect exchange, so money emerges from countless dispersed decisions without central decree⁹. In the metallic age, saleableness came from physical attributes; in the on-chain age, verifiability becomes a critical component of saleableness—whether rules are public and state independently recheckable directly affects whether a token can be accepted across stranger counterparties. White further noted in the *American Economic Review* that what competitive issue most struggles to close is often not note authenticity but unit of account convergence: when multiple private monies coexist, whose price list prevails? Selgin’s (1984) evolutionary model treats clearinghouse discount reflux as a key link for endogenizing discipline under competitive issue—together with Menger’s answer to “what becomes medium,” Mises’ s regression theorem explaining “whence present prices,” and search theory explaining “why acceptance persists in equilibrium,” forming a fourth difficulty¹². In the protocol era, ISO 4217 tickers and VRC-10 multi-fiat units reopen this difficulty at the engineering layer. This aligns with Selgin’s “synthetic commodity money” response to the regression theorem: what markets select is a bundle of attributes that lower transaction costs; in the digital age that bundle must include cryptographically verifiable scarcity and execution. Saleableness ranking and verifiable rules can stand as twin dimensions of monetary emergence in the protocol era—the former explaining why chosen, the latter why strangers can trust.

If “verifiability” is treated as a testable concept rather than rhetoric, at least two observable implications follow. When collateral ratios, reserve composition, and on-chain holdings can be independently rechecked, transmission from reputational shocks to purchasing power should be weaker than for stablecoins relying on black-box reserves—requiring ex post comparison of depeg events and recovery speed, not a priori assertion. When oracles or governance are breached, another boundary appears: “verifiable state” guarantees only in-chain consistency, not off-chain truth—the contagion cascades in Section 3 are counterexamples. Boundaries do not cancel the value of verifiable rules; they show the promise is conditional, not unconditional.

Section 5. Three Changes Hayek Did Not Live to See

Projecting Hayek’s competing-currency framework onto the 2024 blockchain ecosystem, three changes especially deserve separate discussion—the global synchronous ledger, open-source standards, and governance tokens—pushing competing currencies from “philosophical possibility” toward “observable experiment,” while strictly distinguishing possibility from institutional reality.

The global synchronous ledger compresses cross-border verification costs near zero. When Hayek’s competing-currency vision was worked through inside Europe, it already faced barriers to cross-border information transmission and verification: how to know the reserve position of a private bank operating in

another country? Blockchain networks compress that technical cost from “needs a professional investigation agency” to “run a node”—and nodes can run anywhere with internet, unbound by physical distance¹³. In the nineteenth-century U.S. free-banking era, merchants relied on publications such as the *Bank Note Reporter* to authenticate notes and discounts one by one—Rockoff (1974) and Rolnick–Weber (1988) show that institutional detail (bond collateral, parity laws) and information costs jointly determine whether competition can move in the Thiersian direction; Dowd’s clearinghouse model shows that paper-era discount-clearing networks were themselves embryonic “verifiable discipline”—on-chain full nodes structurally fill the same gap, only the medium shifts from paper directories to verifiable state machines¹⁴. Geographic boundaries of monetary competition expand from regional networks (Hanseatic Baltic cities, Scottish banking communities) to the globe; verification thresholds fall from specialized knowledge to computational resources.

Open-source standards simultaneously lower issuance barriers and raise rule observability. Hayek’s envisioned competing-currency issuers were financial institutions with reputation and capital reserves; the issuance barrier itself supplied some quality screening. On-chain, any team with development capacity can deploy a token contract in days; issuance barriers plunge; at the same time, issuance rules are public as open-source code anyone can read, analyze, and criticize. This is a transparency mechanism different from institutional reputation: reputation is *ex post* and fuzzy; code is *ex ante* and explicit. Competitive units can thus shift from banking persons to verifiable rule suites—discipline need not rest entirely on “which bank is more trustworthy,” but can partly rest on “whether rules are independently verified as executed.”

Governance tokens also allocate part of “monetary policy” decisions to holders. In Hayek’s vision, private issuers maintain monetary quality from self-interest; the public can express discontent only by “selling.” On-chain protocols introduce governance-token mechanisms: critical parameters (stablecoin collateral ratios, interest-model parameters, fee-distribution shares) are decided by token vote. Holders are not only passive recipients but potential participants—able to propose, vote, and push change. Though in practice most holders do not actively govern, the mechanism’s existence turns “participating in the issuer’s policy-making” from theoretical possibility into technical reality—a right traditional money holders never had.

Critics often cite on-chain nominal transfer volume, token variety, and DeFi locked value to assert that “monetary competition has loosened monopoly.” That claim must also face metrics such as adjusted on-chain payments as a share of global flows and fiat’s share in taxes and wages (on-chain real payments remain marginal in global payment flows—three metrics and data in Chapter 1, Section 8¹⁵); most advanced-economy indicators do not support a “monopoly ended” narrative. Ma et al. (2023) show that stress-period stablecoin flows synchronize highly with crypto-market liquidity; edge-corridor adoption more often reflects exit options when fiat anchors fail than retail legal-tender substitution—to be read with Chainalysis geography reports and IADB El Salvador surveys, not extrapolated from single-chain TVL as institutional turn. Barbon & Rinaldo (2024) further show that CEX/DEX liquidity quality, gas fees, and arbitrage deviations significantly affect peg observability; indicators that “competition is happening” must also include OTC/DEX depth and redemption channels, not only address counts or TVL¹⁶. Surveying free-banking historiography, Kroszner reminds that Scotland is instructive for competitive issue, but extrapolation to the present must distinguish community scale, clearing infrastructure, and legal enforcement—the on-chain global ledger changes information costs but does not automatically change tax anchors and lender-of-last-resort expectations¹². Using nominal transfer volume to prove monopoly broken, and using adjusted shares to deny all technical significance, are alike methodological errors.

If those metrics rise in edge corridors where fiat anchors fail, a more accurate formulation is that competition first occurs at the levels of rule verifiability and participation structure—anyone can deploy tokens, anyone can audit collateral state—this is “dusk,” not “midnight.” El Salvador’s 2021 writing of Bitcoin into legal

tender and promotion of the Chivo wallet is often cited as proof that “monopoly is broken”; a 2022 Inter-American Development Bank survey found only about 12% of surveyed Salvadorans regularly used Chivo, about 70% still mainly relied on cash, and most daily transactions remained dollar-denominated¹⁷—legal status is not actual adoption. Chainalysis’ *2024 Geography Report* shows that high-inflation economies such as Argentina and Turkey have significantly above-global-mean stablecoin on-chain receiving intensity¹⁸—substitution often starts in edge corridors where fiat anchors fail, then seeps toward the mainstream; whether edge seepage becomes institutional normality remains unsettled. Terra/UST’ s 2022 collapse from nearly \$18 billion circulation to zero in days (He et al. 2023 IMF Fintech Note mechanism taxonomy; Ortiz & Witte 2023 run-speed comparison) shows that high TVL and transparent rules can likewise fail fast in competitive experiments—not that monopoly has yielded or protocol discipline has institutional recognition—Li, Meyer & Zlate (2023) Boston Fed ex post analysis reads the 2022 Terra run with the 2023 USDC/SVB run, showing that stablecoins on stress days also exhibit MMF-style flight-to-safety (from riskier stablecoins toward those seen as safer); competition occurs inside the stablecoin spectrum, not as full retail-fiat substitution¹⁹. Mainstream penetration speed depends on compliance interfaces and liquidity depth and cannot be extrapolated from white-paper roadmaps. Unresolved questions remain: advanced-economy retail legal tender and tax anchors will for the foreseeable future still lock to domestic currency; the main battlefield of protocol competition is edge corridors and open-ecosystem internal pricing, not wholesale substitution of global payment flows.

Section 6. The Political Economy of the Global Ledger

The global ledger’ s existence means it falls under multiple legal jurisdictions at once, with no single sovereign able to exercise complete jurisdiction over it. That property is the technical source of its cross-border settlement advantage, the root of regulatory difficulty, and a new variable in global monetary geopolitics.

National authorities’ treatment of crypto assets displays a rare plural spectrum. El Salvador wrote Bitcoin into legal-tender provisions. China banned Bitcoin mining and trading comprehensively, yet the digital yuan (eCNY) project continues—the latter a path of upgrading the public ledger while retaining seigniorage. The U.S. SEC in January 2024 approved the first spot Bitcoin ETFs, bringing Bitcoin into traditional securities distribution channels²⁰; regulatory frameworks for DeFi protocols and stablecoin issuers continue to evolve. The EU Markets in Crypto-Assets Regulation (MiCA) took full effect in June 2024, establishing a relatively unified licensing framework across the EU²⁰—these moves expand investment and compliance interfaces, not automatically institutionalize retail-layer monetary competition.

Such regulatory divergence is itself a form of policy competition: jurisdictions compete via regulatory-environment differences for crypto-related economic activity—exchange operations, protocol development, mining energy procurement, institutional entry. In a sense this is Hayek’ s hoped-for “policy competition” at the national level: though the competitive unit is the regulatory framework rather than money itself, the underlying logic is akin—when exit options (migration to another jurisdiction) exist, policymakers face pressure to remain competitive.

Deeper political-economic tension lies in the structural conflict between sovereign monetary systems and the global ledger. National tax administration depends on visibility and jurisdiction over domestic economic activity; monetary-policy transmission depends on public use of domestic money. Self-custodied crypto assets on decentralized networks, passing through no domestic institution, can move rapidly on-chain when domestic political risk rises—a direct challenge to capital-control systems. That tension will not vanish with technical progress; it will continue to be negotiated in different forms as regulatory frameworks and technical evolution interact.

Section 7. Zero-Knowledge Proofs: Extending the Boundary of Verifiable Rules

The global ledger's verifiability has an important technical boundary: it can verify "what happened on-chain," but cannot directly verify "off-chain reality." Price oracles supply off-chain price data; if manipulated, contracts still execute on wrong inputs and produce wrong results; on-chain identity does not automatically map to real-world subjects; compliance requirements (AML, KYC) need to link on-chain addresses to real identity, structurally conflicting with pseudonymity.

Maturation of zero-knowledge proof (ZKP) technology supplies an important tool for extending the boundary of verifiable rules. ZKPs allow a prover to convince a verifier that "a statement is true" without revealing the underlying information. For example: prove "I am over 18" without disclosing age; prove "my balance exceeds a threshold" without disclosing the balance; prove "this transaction's origin meets compliance requirements" without disclosing transaction history.

The monetary-policy implications are deep. In traditional systems, compliance (identity, source tracing) and privacy trade off: to comply, disclose; to protect privacy, struggle to comply. ZKPs technically allow both: users can "prove conditions are met" to compliance parties without exposing concrete data. ZKPs have not fully resolved the tension—implementation remains complex and costly, and legal frameworks have not fully accepted ZKP proofs' compliance force—but at the technical layer they open the possibility that "compliance need not equal nakedness," supplying tools for verifiable rules to find a new balance between privacy and regulatory compliance.

ZKPs can also extend blockchain scaling paths. ZK Rollup technology moves computation for large volumes of on-chain transactions off-chain, submitting only compressed validity proofs on-chain while retaining the same security guarantees as the main chain—anyone can verify the proof that all off-chain computation followed the rules, without re-executing every transaction. Throughput rises sharply while core attributes of verifiable rules are preserved. ZK Rollup schemes in the Ethereum ecosystem (such as zkSync and StarkNet) are concrete realizations of this path and represent the technical frontier of verifiable rules on the scalability dimension.

Section 8. Bitcoin's Lightning Network: Extending Verifiable Rules toward Scaling

Bitcoin's base-layer limit of seven transactions per second is a deliberate design choice: smaller blocks help keep full-node operating costs within individual reach, preserving network decentralization. Yet that choice prevents Bitcoin from directly meeting global retail-payment throughput needs, giving rise to "Layer 2" solutions—the Lightning Network.

Proposed in 2016 by Joseph Poon and Thaddeus Dryja, Lightning's core idea is to open an off-chain payment channel between two users: both lock some bitcoin in an on-chain multisig contract, then freely make any number of instant small payments inside the channel, settling final state on-chain only when the channel closes. Channels can interconnect into a network so users without a direct channel can pay via intermediate routing nodes.

This design extends the concept of "verifiable rules": every in-channel state update carries signatures; if either party tries to broadcast an outdated state (cheat-closing the channel for more funds), the counterparty can broadcast a "penalty transaction" before the timelock expires and confiscate all channel funds. The penalty mechanism turns "not cheating" into a self-enforcing incentive—the cost of cheating is clear and immediate, without depending on judicial process. This is a concrete case of "rules as law" on-chain: contract logic replaces contractual dispute resolution; incentives replace moral constraint.

Lightning supplies a technical path for Bitcoin in everyday micropayments; El Salvador's Chivo wallet once used it as backbone, but adoption remained limited. Large routing depends on deep enough channel liquidity; channel open/close still requires on-chain transactions; routing failures and self-custody thresholds hinder ordinary-user adoption. The gap between technical foundation and everyday experience must be measured by penetration, failure rates, and merchant acceptance, not extrapolated from white-paper roadmaps as accomplished reality.

Section 9. New Dimensions of Programmable Money: VRC Protocols and Protocol-Layer Standards

Bitcoin answered "can an immutable monetary ledger be built"; Ethereum answered "can plural tokens and programmable financial logic be supported within a standardized framework." After Ethereum, application-specific chains and protocol layers continually emerge, seeking different balances in the "decentralization, security, scalability" triangle.

The VRC (Versatile Resource Coin) protocol suite proposed on the Openverse network is an engineering attempt to encode "rules encodable, issuance auditable" as concrete interfaces—to be stated clearly as a design vision, still awaiting scaled operation, courtroom practice, and independent audit, not to be treated as a production monopoly substitute. VRC-10 (Bitcurrency) intends to supply a public-domain stable unit of account, relying on PCIM (Public Currency Issuance Mechanism) for overcollateralized competitive minting; VRC-11 (Privcurrency) targets permissioned private-domain stable settlement; VRC-12 is positioned as a security-type token rather than medium of exchange. Collateral ratios, upper bounds on peg deviation, and welfare implications of competitive issue belong to stability-mechanism topics; here the only questions are whether issuance parameters are on-chain readable and whether state can be third-party rechecked.

VRC-20 is close in spirit to Ethereum's ERC-20 (fungible-token standard enabling any contract to issue interoperable tokens), intending to lower migration costs. Differences lie mainly in underlying resource pricing: Ethereum signals computational scarcity with gas fees; Openverse's energy and bandwidth model supplies another allocation logic—which better serves monetary competition awaits deployment data, not white-paper assertion. The VRC suite is a re-implementation on a specific architecture, not a simple copy of ERC-20; whether it becomes a reference case on the popularization path depends on mainnet operation, compliance landing, and whether peg mechanisms withstand stress tests—none of the three has yet closed verification.

Section 10. The Global Ledger as Technical Foundation

Hayek's competing-currency vision, in his writing years, was constrained by information asymmetry, switching costs, the reach of reputation mechanisms, and lack of technical infrastructure—objective limits of technical conditions, not errors in the idea itself. The global ledger and verifiable rules are the foundation on which, after a qualitative shift in the supply curve of those conditions, competing currencies move from philosophical vision toward engineering practice.

The global ledger and verifiable rules constitute the technical foundation of monetary popularization; they are not yet popularization itself. The foundation makes popularization theoretically feasible, but making it truly well used still requires extensive subsequent work in protocol design, governance structure, legal frameworks, and social consensus. From Bitcoin's hard constraints, through Ethereum's programmable issuance, through the VRC suite's multi-asset standards, to ZK proofs' extension of privacy and compliance boundaries, each step enriches the meaning of "verifiable rules." The aim of this evolutionary series is to give trust a firmer, more transparent, more accountable foundation—also the deepest institutional meaning of "monetary popularization."

The global ledger also brings a knowledge public good that did not previously exist: complete on-chain transaction history. Academic researchers, regulators, and risk assessors can all access the full record of all historical transactions on Bitcoin or Ethereum and conduct monetary-economics research at scales far beyond traditional financial archives. Who holds, how funds flow, holder behavior under different price shocks—questions hard to study independently in traditional finance because of data privacy are open to everyone on-chain. This democratization of knowledge is itself a component of monetary popularization: not only participation in issuance, but also real understanding of how monetary systems work and independent analytical capacity.

An often underestimated layer: the value of verifiable rules ultimately appears in holders' willingness to believe rules will be obeyed, and ability to recognize and exit when they are violated. Technical verifiability supplies capability; it cannot automatically create willingness and cognitive capacity. Most money holders will not personally run full nodes to check the ledger; they rely on trusted middle layers—wallet providers, exchanges, media—to perceive whether verifiability truly exists. That means the global ledger's value depends not only on technical infrastructure but also on information-propagation mechanisms and user education. For the promise "rules over persons" to land, it ultimately depends on participants' depth of understanding and capacity to exercise that promise. That is the social dimension of monetary popularization beyond technology.

注释与引用

1. Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System," §4 (PoW cites Back Hashcash); Back (2002), "Hashcash - A Denial of Service Counter-Measure," §§1–3. <https://bitcoin.org/bitcoin.pdf> ; <http://www.hashcash.org/papers/hashcash.pdf> ↩
2. Wei Dai (1998), "b-money" (distributed ledger, proof of work, and anonymous participants; credited in Satoshi Bitcoin white paper References); Easley, O'Hara & Basu (2024), "From mining to markets: The evolution of bitcoin transaction fees," *Journal of Financial Economics* 169, 103892: after block-reward decline, fee markets become the main miner-incentive channel. <https://www.weidai.com/bmoney.txt> ; <https://doi.org/10.1016/j.jfineco.2024.103892> ↩
3. Szabo (2005), "Bit gold"; Szabo (1998), "Secure Property Titles with Owner Authority" (distributed property registration); Finney (2004), "Reusable Proofs of Work (RPOW)" (engineering middle link for bit gold); Narayanan et al. (2016), *Bitcoin and Cryptocurrency Technologies*, Princeton, Ch. 1–2 (P2P ledger survey). <https://nakamotoinstitute.org/secure-property-titles/> ; <https://nakamotoinstitute.org/library/finney-rpow/> ; <https://bitcoinbook.cs.princeton.edu/> ↩
4. Hayek, 1976, *The Denationalization of Money*, ch. 8 "The Future of Private Coinage?" on competitive circulation of private paper; ch. 11 pp. 46–47 "Control of the Value of Competitive Currencies": issuers must "keep their (precisely defined) purchasing power as nearly as possible constant." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
5. Buterin (2014), *Ethereum White Paper*, §§"Ethereum Accounts" and "Applications": Turing-complete state machine + smart-contract execution environment (official white paper, not independently audited); Wood, Gavin, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Yellow Paper, §§1–2 (state-transition system), §4.2 (Gas metering); Szabo (1997), "Formalizing and Securing Relationships on Public Networks," *First Monday* 2(9): smart contracts as automatically executable relational protocols. <https://ethereum.org/en/whitepaper/> ; <https://ethereum.github.io/yellowpaper/paper.pdf> ; <https://firstmonday.org/ojs/index.php/fm/article/view/548> ↩ ↩²
6. CoinSchedule, *ICO Stats 2017*: ~\$5.6 billion raised in token sales, 1,000+ projects; Fabric Ventures / Atomico, *State of European Tech 2017* also summarizes contemporaneous scale. Scope includes private and public presales; post-fraud share: U.S. SEC enforcement notices and academic ex post studies (e.g. Howell et al., 2020). ↩
7. Euler Finance attack: BlockSec / PeckShield on-chain tracing, 2023-03-13 losses ~\$197 million; Mango Markets (2022-10), Curve (2023-07) oracle-manipulation cascades: protocol post-mortems and Chainalysis incident analyses. ↩
8. Mises, 1949, *Human Action*, pp. 257–260 (economic calculation problem): price signals carry dispersed knowledge; calculability is a premise of rational resource allocation. English: <https://www.econlib.org/library/Mises/HmA/msHmA.html> ↩

9. Menger, 1892, *On the Origin of Money*, §§1–2 (saleableness ranking; §1 "wirtschaftlichsten Güter" = most easily disposed goods pushed into indirect exchange); English: https://cdn.mises.org/On%20the%20Origins%20of%20Money_5.pdf ↩ ↩²
10. Kiyotaki, Nobuhiro, and Randall Wright. "On Money as a Medium of Exchange." *Journal of Political Economy* 97(4), August 1989, pp. 927–954 (formal precursor of saleableness ranking under search frictions); Kiyotaki & Wright, "A Search-Theoretic Approach to Monetary Economics." *American Economic Review* 83(1), March 1993, pp. 63–77 (intrinsic vs extrinsic saleableness; read with Menger §§1–2, Mises ch. 8 regression theorem). <https://doi.org/10.1086/261634> ; <https://doi.org/10.1257/aer.83.1.63> ; cross-ref. ch07 §6 [^31]. ↩ ↩²
11. Szabo (2002), "Shelling Out: The Origins of Money" (collectibles cooperation and monetary collaboration origins); Szabo (2017), "Money, Blockchains, and Social Scalability": "Social scalability is the ability of an institution ... to overcome shortcomings in human minds ... that limit who or how many can successfully participate" (social scalability—verifiable rules substitute for interpersonal trust costs); cross-ref. Chapter 7, Section 6 [^22], Chapter 20, Section 9, [glossary.md](#) "verifiability." <https://nakamotoinstitute.org/shelling-out/> ; <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↩
12. Selgin, George, "The Evolution of a Free Banking System," *Economic Inquiry* 22(3), July 1984, pp. 289–300 (clearinghouse discount reflux); White, Lawrence H., "Competitive Payments Systems and the Unit of Account," *AER* 84(3), 1994, pp. 699–712; Kroszner, Randall S., "Free Banking: The Scottish Experience as a Model for Emerging Economies?" *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31. ↩ ↩²
13. Hayek, 1976, *The Denationalization of Money*, p. 23: the competitive scheme aims so that issuers of bad money "at once lead to the rapid displacement of the offending currency by others." PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
14. Rockoff, Hugh, "The Free Banking Era: A Reexamination," *JMBC* 6(2), 1974, pp. 141–167 (*Bank Note Reporter* and interstate discount circulation); Rolnick & Weber, "New Evidence on the Free Banking Era," *AER* 78(5), 1988, pp. 880–890; Dowd, Kevin, *Laissez-Faire Banking*, Routledge, 1993, ch. 2–4 (clearinghouse-endogenized discipline). ↩ ↩²
15. Stablecoin three metrics (nominal flow, Visa-adjusted, McKinsey real payments ~0.02%): see Chapter 1, Section 8 footnotes 1714. ↩
16. Barbon, Andrea, and Angelo Rinaldo (2024), "On the Quality of Cryptocurrency Markets: Centralized versus Decentralized Exchanges," *Management Science* forthcoming; arXiv:2112.07386: CEX/DEX liquidity quality, gas fees, and arbitrage deviations—competition metrics must include market depth, not only on-chain nominal volume. He, Dong, Ross Leckow, Tommaso Mancini-Griffoli, and Hiroshi Nagaoka (2023), IMF Fintech Notes 2023/001: stablecoin mechanism taxonomy and run risk; Ortiz & Witte (2023), BIS WP 1137: algorithmic vs overcollateralized run speed. Complementary to Ferraro, Kan & Sunderam (2022) thin-market peg analysis. <https://arxiv.org/abs/2112.07386> ↩
17. Inter-American Development Bank (2022), "Survey on the Use of Bitcoin in El Salvador": ~12% regular Chivo use, ~70% still mainly cash; Liu et al. (2023) NBER WP 31160: Terra on-chain sophisticated-first exit. <https://www.iadb.org/en/news/survey-use-bitcoin-el-salvador> ↩ ↩²
18. Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*: Argentina, Turkey, Venezuela and other high-inflation economies show significantly above-global-mean stablecoin receiving intensity; edge-corridor adoption, not automatically extrapolated to advanced-economy retail. <https://www.chainalysis.com/blog/2024-geography-of-cryptocurrency-report/> ↩
19. Li, Ye, Stephen Meyer, and Andrei Zlate (2023), "Runs and Flights to Safety: Are Stablecoins the New Money Market Funds?," Federal Reserve Bank of Boston Research Series SRA 2302 (2022 Terra run and 2023 USDC/SVB run flight-to-safety contrast; competition inside the stablecoin spectrum, not full fiat substitution). <https://www.bostonfed.org/publication/s/research-special/2023/runs-and-flights-to-safety-are-stablecoins-the-new-money-market-funds> ↩
20. U.S. SEC, 2024-01-10 approval of first spot Bitcoin ETFs (Rule 10b-1 effective); EU MiCA (Regulation EU 2023/1114) stablecoin and CASP provisions fully applicable from 2024-06-30. Compliance-interface expansion, not change in retail legal-tender status. ↩ ↩²

§ 7 Money and the State in Classical Economics

The global ledger answers “how to enforce rules,” not yet “what economic philosophy rules should obey”—classical economists argued that question for three hundred years.

Monetary questions run through three centuries of Western economic thought, from Smith’s awe at the efficiency of the division of labor, to Ricardo’s pursuit of the value of coinage, to Keynes’s rediscovery of effective demand, to the Austrian school’s distinctive understanding of monetary order—each generation wrestled with the same problem: whose is money, who governs it, and can it be deliberately managed? When blockchain protocols rebuild the technical base of monetary issuance, which classical presumptions long treated as natural laws do they unsettle?

Every major turn corresponds to an institutional crisis in the real world: Ricardo’s metallism answered post-Napoleonic inflation; Keynes’s demand management answered the Great Depression; Friedman’s monetarism answered stagflation; the Austrian theory of competing currencies answered the systemic failure of state monetary monopoly. Reading these crises against their intellectual responses clarifies blockchain protocols’ place in the history of monetary thought: they continue a continuous chain of intellectual exploration and technically supply rule verifiability that the paper-money era could scarcely achieve—whether institutional consequences cash out as particular answers must still be checked against observable metrics, not treated as a technological miracle descending from nowhere.

Section 1. Smith’s Logic of Division of Labor and the Origin of Money

Adam Smith opens Chapter 4, “Of the Origin and Use of Money,” Book I of *The Wealth of Nations* (1776), with the pin-factory story: ten workers in divided tasks can make nearly forty-eight thousand pins a day; if each completed the whole process alone, twenty pins a day would be hard to guarantee. The productivity leap from division of labor astonished Smith, but he immediately asked: division means each worker produces what he does not himself consume; all must exchange surplus for others’ surplus—what lubricates that exchange? Money thus enters Smith’s theoretical field: it is not wealth itself, but the medium that lets the division of labor keep running over wider geographic range.

Smith’s narrative of monetary origins has a distinctly evolutionary cast. In a barter state, people soon meet the harsh requirement of a “double coincidence of wants”: your fish must be what he wants for his cloth, and he must want fish—such coincidence grows rarer as population densifies and specialization deepens. Market participants therefore spontaneously converge on some generally accepted commodity—an “intermediate good” everyone will take even without direct use. Societies tried cattle, shells, iron, tobacco, salt; gold and silver finally won through durability, divisibility, portability, and resistance to decay. Carl Menger systematically argued the same logic in *On the Origin of Money* (1892): money is a spontaneous order that emerges when the most “saleable” commodity is selected through countless dispersed exchanges, not a product of state decree¹.

Worth close reading is that Smith did not credit monetary-value stability to state sovereignty. He distinguished “nominal price” from “real price”: real price is determined by the toil of labor expended in production; money is merely the measuring rod of labor. His attitude to Bank of England notes was conditional approval—so long as notes maintained metallic convertibility and were not overissued, they differed in essence little from coin and were more portable, favoring commerce. But once bankers, driven by profit, overissued, money turned from lubricant into destroyer. Government’s role should be to make and enforce rules against overissue, not to become the overissuer.

Here already lies a lasting tension: money is in essence a spontaneous market product, yet market operation also needs institutional guarantee of monetary rules. Smith did not systematically resolve that tension; successors extended it in different directions and finally split into metallists, quantity theorists, Keynesians, and Austrians—giving sharply different answers to the same question.

Chartalism approaches the same problem by another path. Knapp in *The State Theory of Money* (1905) and Innes in “What is Money?” (1913) argue that in the modern fiscal state, monetary value is primarily anchored in state acceptance of taxes and legal-tender commands, not in commodity saleableness rankings—“acceptance circles” are often first drawn by taxation and legal status; Mengerian emergence narratives better explain metallic-era origins than the everyday sanctity of today’s fiat². Goodhart summarizes the split as two concepts: M-money (market money of account) and C-money (state money of account): in modern fiat they overlay and coexist rather than mutually exclude—Zimbabwean and Argentine high inflation show that the C-money circle can maintain tax-nominal demand while M-money ranking has already shifted to the dollar³. This path does not mean to deny Menger’s archaeological narrative of the metallic age, yet it warns: on-chain verifiability can compress information costs of issuance rules without automatically expanding the acceptance circle—if protocol tokens have not entered the main loops of tax, wages, and public procurement, competition may long remain in edge corridors. Three intellectual-historical threads—Mengerian emergence, the chartalist state anchor, and Hayekian competition—must all be taken into the protocol era, not one chosen to the exclusion of others.

Section 2. Ricardo’s Metallism and Rules First

Ricardo followed Smith with a sharper stance on money. What drove him deep into monetary theory was a concrete policy crisis: during the Napoleonic Wars the British government needed continuing war finance; from 1797 the Bank of England suspended specie convertibility; note supply expanded sharply; sterling’s external exchange rate fell heavily; domestic prices rose. The episode sparked fierce public debate; Ricardo entered with *The High Price of Bullion* (1810) and related essays, becoming a leading voice of the “Currency School.”

Ricardo’s core claim: paper inflation is essentially a hidden tax levied by government on all money holders. Victims are creditors and workers holding fixed nominal assets; beneficiaries are debtors and issuers—especially government itself. This redistribution of wealth is completed through increase in money quantity rather than legislative procedure, thus needing no explicit parliamentary approval; monarchs and governments historically never resisted it.

Ricardo’s policy prescription was therefore extremely simple: money supply should follow predictable rules, not the discretion of bankers or politicians. The labor cost of gold mining supplied an objective benchmark for monetary value; metallic convertibility was the institutional chain constraining paper overissue. He supported the spirit of Peel’s Act (1844): requiring new Bank of England notes to be backed by equal specie reserves—in substance taking issuance power back from bankers and handing it to near-natural hard constraints.

Yet metallism has inherent fragilities Ricardo seems to have underestimated. The gold standard did provide price stability in normal times, but when financial panic swept, runs forced banks to contract credit, amplifying deflation and real collapse together. The British financial crises of 1847, 1857, and 1866 were each survived by suspending Peel’s Act and allowing excess note issue. The contradiction between rules and crises—the eternal game of elasticity and constraint—has no elegant exit in Ricardo’s system.

That contradiction reappears two centuries later in Bitcoin debates, with strikingly similar structure: a fixed issuance cap remains persuasive against inflation narratives, but when the macro environment needs elastic response, the cost of algorithmic rigidity is equally hard to dodge. Historical context changed; the structure of institutional tension remains the same.

Section 3. The Quantity Theory of Money: From Hume to Fisher

Long before Ricardo's century, the Scottish philosopher David Hume had systematically stated the quantity theory's basic proposition. In a 1752 essay he ran a thought experiment: suppose one night every Briton found five extra pounds under his pillow—he inferred no one would be truly richer; prices would merely double, because goods were unchanged while money chasing them had doubled. Money is a "veil," altering only the nominal price scale, not the intrinsic ratios of real exchange—the earliest clear statement of so-called "monetary neutrality."

Irving Fisher algebraized the proposition in *The Purchasing Power of Money* (1911), giving the famous equation of exchange: $MV=PT$. Money stock (M) times velocity (V) equals price level (P) times transactions (T). As an accounting identity the equation is logically airtight, but once auxiliary assumptions are added—"V stable in the short run, T determined by real production conditions"—it becomes a powerful policy proposition: control money stock and you control prices. The monetary authority's duty thus emerges—it should manage money supply to prevent inflation from too much money chasing too few goods.

The quantity theory met Keynes' s fierce assault in the first half of the twentieth century and was restored in the middle and later decades by monetarism under Milton Friedman. Friedman' s contribution was not only to defend the quantity theory but to refine inflation from a vague social phenomenon into "too much money chasing too few goods." *A Monetary History of the United States* (1963), coauthored with Anna Schwartz, supplied a new analytical frame for historical research: every major monetary contraction accompanied recession; the root cause of the 1929 Great Depression lay not in capitalism' s inherent defects but in the Federal Reserve' s allowing money supply to contract by one-third between 1930 and 1933⁴—over the same span U.S. nominal GDP fell from about \$104 billion to \$76 billion (1929–1933), and unemployment peaked near 25% in 1933⁵. That diagnosis overturned mainstream narratives of the Depression and founded Friedman' s influence for decades afterward.

The quantity theory itself does not directly support the existence of a central bank. Its most austere policy implication is: maintain predictable money-supply growth; no complex institution actively performing stabilization is required. Late in life Friedman repeatedly expressed distrust of the Fed, holding that central-bank discretionary disturbance often exceeded its stabilizing effect. Tension between the quantity theory and central-bank institutions in some measure runs through the entire twentieth-century monetary-policy debate.

The quantity theory also has an underestimated epistemological significance: it was the first major attempt to convert monetary-policy propositions from moral discourse into quantitative propositions testable by empirical data. Before Hume and Fisher, discussion of money was mainly normative—kings should not debase coin; governments should not overissue paper. Converting those judgments into "systematic relations between M growth and P change" was a step in economics' establishment as a scientific discipline. That methodological importance is no less than its specific theoretical content—it founded the tradition of constraining monetary-policy discussion with quantitative evidence; on-chain protocols advance that tradition at the level of parameters publicly readable and historically replayable—whether that therefore beats central-bank discretion still depends on institutional adoption and observable results, not on the mere existence of code.

Section 4. The Keynesian Revolution: The Politicization of Money

When John Maynard Keynes published *The General Theory of Employment, Interest and Money* in 1936, the world economy had been mired in the Great Depression for over five years. Before idle factories and unemployment queues, the classical advice to wait for wages to fall automatically and markets to clear naturally had become politically and morally untenable. Keynes offered a sharply different diagnosis: the root was not wage rigidity but systematic deficiency of effective demand.

Keynes established the separation of saving and investment as the core clue to understanding fluctuations. In classical economics, saving automatically becomes investment; the interest rate is the price signal balancing the two. Keynes argued: when agents are broadly pessimistic about the future, even lower interest rates will not induce investment—expected demand is already weak; new capacity only deepens losses. More fundamentally, money has the “liquidity preference” Keynes systematically elaborated in Chapter 13 of *The General Theory* (1936): in uncertain times people choose to hoard money rather than spend; such collective behavior compresses effective demand and stalls the economy at a low-employment equilibrium, while market price mechanisms have no self-correcting power against it.

Monetary policy has inherent limits in this framework. When interest rates already near zero, further easing neither lowers real borrowing costs nor activates investment willingness—Keynes’ s “liquidity trap.” In that case fiscal expansion—government spending directly, creating demand—becomes the only tool that can break the deadlock. Monetary and fiscal policy thus enter a framework of coordinated cooperation; their boundary becomes highly elastic.

The Keynesian revolution’ s impact on monetary institutions was deep and lasting. It gave theoretical legitimacy to active government intervention, requiring the central bank to act as an active macro stabilizer in crises rather than a passive machine executing money-supply growth rules. Monetary-policy goals expanded from “maintain convertibility” gradually to “achieve full employment and price stability”—the appearance of a dual mandate means the central bank must make hard trade-offs, and those trade-offs are essentially political. Money was no longer a neutral veil but a policy tool that can be actively used to change real outcomes. That cognitive shift founded the intellectual basis for postwar decades of central-bank institutional expansion.

Since the late twentieth century, Woodford, Galí, and others have woven the Keynesian liquidity trap and Friedmanite expectation anchoring into a New Keynesian synthesis: downward rigidity of nominal wages and some prices makes moderately positive inflation (about 2%) welfare-superior and buffers the effective lower bound (ELB) constraint; flexible inflation targeting (FIT) then folds the employment gap into the central bank’ s reaction function, claiming to internalize distributional concerns within a discretionary framework⁶. The DSGE benchmark models of Christiano–Eichenbaum–Evans (2005) and Smets–Wouters (2007) supply estimable impulse responses for this framework—lag paths of monetary-policy shocks on output and inflation became quantitative references for central-bank communication and forward guidance⁶. This framework is orthogonal to the protocol path: if FIT remains one of the optimal macro stabilizers within sovereign fiat systems, what is contested is whether mint participation rights must be closed, not wholesale denial of countercyclical tools. CBDC literature pushes the same tension back to the transmission side: Holston, Laubach, and Williams (2017) estimate advanced-economy natural rates r^* fell from about 3%–4% in the 1980s to near zero in the 2010s; BIS (2023) cross-country summaries show r^* highly sensitive to model specification—low- r^* environments compress traditional rate-cut space, making Brunnermeier and Koby’ s (2019) “reversal rate” and Bindseil’ s (2020) tiered CBDC design companion issues for FIT in the ELB era, not macro stabilizers that protocol money can replace⁷.

Section 5. Friedman and Monetarism: Rules versus Discretion

Under the monetarist banner Friedman launched a systematic rebuttal of the postwar Keynesian discretionary tradition. His core proposition can be summarized: monetary policy’ s lag runs from half a year to two years and is highly uncertain in length; under those conditions every central-bank attempt at “precise fine-tuning” is in fact a delayed response to a reality that has already changed, often pouring fuel rather than water. Discretion is not only useless; it actively manufactures fluctuations.

1970s stagflation—high inflation and high unemployment together, the Keynesian Phillips curve failing—became monetarism’s historical case. As early as 1968 Friedman had predicted that if government tried to buy employment with inflation, workers’ inflation expectations would adjust accordingly; real-wage falls would be offset by nominal-wage rises; the short-run “employment-for-inflation” trade would necessarily unravel in the medium and long run, leaving both worse. That prediction’s fulfillment is among the most powerful theoretical tests in twentieth-century monetary economics.

Friedman himself advocated constraining money growth by a “k% rule”—whatever the cycle, increase money supply by a fixed proportion each year (about 3%–5%). Not optimal strategy, but predictable and accountable, avoiding systematic bias from decision-makers’ subjective judgment. In his vision the central bank should not be seen as a clever macro-control machine but as an organization that must be strictly rule-constrained to prevent “good intentions doing harm.”

Yet Friedman’s monetarism also has historical limits: he advocated rules but accepted the central bank’s existence; he criticized discretion but believed that once institutions were well designed, the central bank could be an effective rule executor. He lacked Hayek’s radicalism—he did not advocate abolishing legal monopoly of money issue, still less imagine private or protocol-layer competing currencies⁸. Taylor (1993) operationalized Friedman-style rule preference as the Taylor rule—systematic reaction to inflation and output gaps—becoming the empirical benchmark of the New Keynesian “science” summarized by Clarida–Galí–Gertler⁹; Sargent–Wallace (1981) warned from the fiscal end: under high deficits, lasting low rates accommodating fiscal policy must eventually cash out debt dilution in higher inflation¹⁰. Leeper (1991) further formalized fiscal–monetary regime combinations: under “active fiscal, passive monetary” equilibrium, public-debt expansion is more likely cashed out in inflation than tax adjustment—aligned with the “ends of four big inflations” narrative Sargent (1982) summarized: ending hyperinflation often requires fiscal reform and monetary-anchor rebuilding together, not technical rules alone¹⁰. This is where he diverges from the Austrian tradition, and why his theory still has reference value in the protocol era but is not alone sufficient to prescribe protocol-era policy.

Section 6. Menger and Mises: Money as a Product of Market Process

The Austrian school takes Carl Menger as intellectual founder. Menger’s classic 1892 essay *On the Origin of Money* starts from a sharp proposition: money is not a product of state decree but a spontaneous order emerging from countless dispersed decisions of market participants. His argument path: everyone in barter has incentive to choose the most “saleable” commodity as intermediate medium of exchange—not because a king commands it, but because doing so lowers exchange friction and raises the probability of obtaining what one truly wants. As more people use the same commodity as intermediary, that commodity’s “moneyness” self-reinforces and finally, without any central coordination, evolves into generally accepted money.

The policy implication of this insight is more radical than it first appears. It means the state’s declaring something legal tender is not the source of monetary nature, but only ex post confirmation or forced solidification of what the market has already done. Money’s legitimacy comes from users’ voluntary acceptance, not political authority’s grant. If market participants have better substitutes, legal compulsion is the only means of maintaining monopoly—precisely what Hayek later proposed to break.

Ludwig von Mises greatly extended Austrian monetary theory in *The Theory of Money and Credit* (1912) and introduced analysis of monetary intervention’s dynamic consequences. The core insight of his business-cycle theory: when the central bank injects credit into the banking system at artificially low rates below market equilibrium, price signals received by producers and consumers are distorted—credit ease appears to mean abundant social saving, suitable for launching long-term capital-intensive projects. Mises characterized such

expansion as prosperity driven by “circulation credit,” whose necessary end is liquidation of malinvestment and recession¹¹. Yet such “prosperity” rests on false saving signals; once credit expansion slows, true time preference is revealed and large volumes of malinvestment must be liquidated. Recession here is the endogenous result of artificial boom, not an exogenous shock.

Mises’ s theory draws a fundamental critical boundary around monetary interventionism: the problem is not only whether the central bank’ s technical operations are clever, but that the central bank’ s existence itself necessarily introduces systematic distortion of price signals. Such distortion cannot be eliminated by more clever rule design; it is inherent in the act of concentrated decision intervening in the price process. The Austrian school therefore maintains deep suspicion of all forms of monetary sovereign intervention, whether the intervener is government, central bank, or international monetary organization.

Menger’ s saleableness and Mises’ s regression theorem: tension inside the Austrian school

Menger and Mises appear to share the Austrian tradition on monetary origins, yet there is a often-overlooked fissure. Menger’ s 1892 argument almost does not rely on “nonmonetary use value”: people choose the most saleable commodity as medium because it is easiest to dispose of in exchange—attribute ranking (durable, divisible, broad demand) alone can drive emergence; state decree is only a later overlay¹. Mises in Chapter 8 of *The Theory of Money and Credit* requires: to explain today’ s purchasing power, one must trace history back to a point when the thing was still demanded as an ordinary commodity; otherwise price formation is epistemologically “unanchored”¹². The regression theorem is thus a hermeneutic tool—answering “whence present prices”—not Mengerian selection dynamics—answering “what more easily becomes medium.” Kiyotaki and Wright’ s search-theoretic monetary models supply a formalizable third language for this fissure: in random-matching economies, extrinsic saleableness (belief in wide acceptance as medium) alone can sustain monetary equilibrium even without industrial use—aligned with Mengerian ranking logic; but if one asks how first-day prices enter the exchange network, the regression theorem and “synthetic commodity” path must still answer the historical-anchor question¹³. White and Selgin’ s 1994 *Journal of Economic Literature* dialogue adds a fourth question: even if saleableness solves medium selection, how does the unit of account converge among coexisting monies—whose price list prevailed in the private-banking era is the same class of difficulty as Bitcoin’ s fifteen years of “strong store of value, weak unit of account”¹⁴.

Applying both at once to Bitcoin and on-chain tokens, tension appears immediately: the Mengerian path allows “saleableness ranking” to reopen on digital attributes (verifiable scarcity, global transfer); the regression path asks what priced the first day—if one insists on tracing to nonmonetary commodities, on-chain native assets forever “miss a link” in origin narrative. Wei Dai’ s b-money (1998) and the Hashcash/timestamp chain embedded in Satoshi’ s white paper §§1–4 supply engineering closure of “verifiable scarcity + distributed ledger,” yet do not automatically answer how Mengerian acceptance circles expand—Selgin’ s “synthetic commodity money” (2015) tries to suture: replace metallic physical attributes with verifiable fixed supply and censorship resistance, so Bitcoin functionally meets the regression chain’ s equivalent role without copying commodity history¹⁵¹⁶. Szabo in “Shelling Out” (2002) argues origins of monetary collaboration from prehistoric collectibles cooperation; in “Money, blockchains, and social scalability” (2017) he defines social scalability as the core metric of whether blockchain money can substitute interpersonal trust costs with verifiable rules—aligned with the “verifiability” dimension discussed in Chapters 6 and 20¹⁷. A more cautious reading distinguishes three questions: how zero-price starting points enter the first exchange (historical explanation); given an already formed quote network, what attributes maintain saleableness (ongoing competition); when multiple units coexist, how pricing and clearing coordinate (accounting convergence). Bitcoin’ s fifteen years of market data answer ongoing

competition while making historical explanation a continuing debate—more relevant to Hayek’ s concern that “competition discovers discipline”: discipline comes from testable ongoing survival, not from waiting for full agreement on origin doctrine.

One can thus extend the Mengerian line: one core dimension of saleableness in the digital age is verifiability—whether rules and state can be third-party rechecked at low cost. This need not contradict the regression theorem, but warns not to use origin theorems to deny already running competitive processes; nor to use Mengerian emergence to bypass the hard problems of first-day pricing and ongoing pegs—overcollateralization and redemption mechanisms as white papers envision still await mainnet and stress-event tests, and cannot close pegs by appeal to “spontaneous acceptance” alone.

Free-banking historiography is likewise not a one-sided narrative. White and Selgin, from Scottish experience, stress that option clauses, clearinghouse networks, and discount clearing can endogenize discipline; Calomiris and Haber in *Fragile by Design* (2014) explain from political bargain: frequent early U.S. banking crises partly stemmed from states treating bank charters as political spoils and local financing tools, not from “competition itself necessarily degrading”¹⁸. Selgin’ s 1986 “legal restrictions theory” asks: under layered branching bans, parity laws, and the 1865 holding tax, could markets display the Thiersian direction—reading three explanations together is closer to the sources than binary “free banking good/bad” camp-taking¹⁹. Rockoff and Rolnick-Weber’ s quantitative studies further show: under no forced parity, the direction of bad notes discounting and good notes retained aligns with Thiers; once legislation bans discounting or forces face acceptance, the Gresham mechanism may re-embed in private systems. The two historiographical explanations are not mutually exclusive—they warn that the protocol era must ask simultaneously: can open access lower quality-authentication costs, and can on-chain governance avoid rules being captured by politics or capital. Technology lowering information costs is one thing; whether institutions move in the Thiersian direction remains a proposition.

Section 7. Hayek’ s Competing-Currency Theory: Breakthrough and Limits

Hayek’ s 1976 *The Denationalization of Money* offered in his later years the most radical concrete proposal on monetary institutions: abolish government’ s legal monopoly of money issue; allow private institutions freely to issue their own named currencies; the public freely chooses among multiple currencies by purchasing-power stability. Good money—private monies that maintained stable value—would attract more users; bad money—those that overissued and depreciated—would be abandoned by the market. Competitive pressure forces every issuer to maintain purchasing-power discipline, just as competition in goods markets forces firms to maintain quality. The same cases can be read under three threads—chartalist sanctity peeling away, Thiersian M-money ranking, and limits of Hayekian competing currencies—cross-referenced with Chapter 5, Sections 1–2 and Chapter 2, Section 5 (Zimbabwe’ s three readings), not choosing one to the exclusion of others²⁰.

Hayek explicitly acknowledged in the book that the scheme faced severe practical difficulties. The institutional-premise division of Thiers and Gresham is in Chapter 5²¹²². Competing-currency theory’ s core tension: when multiple private monies coexist and the public cannot identify quality at low cost, spend bad, keep good can still appear; the trigger is authentication information asymmetry, not legal parity²³. Opening competition does not automatically equal low-information-cost competition; private issuers also lack a central-bank lender of last resort²⁴.

Hayek’ s core claim: no central institution holds enough dispersed information to determine money quantity optimally; market dispersed competition is in principle superior to centralized decision, and the monetary domain is no exception²⁵. The institutional conditions he presupposed—issuers constrained by competition, the public

able to monitor monetary quality in real time—were generally missing in the 1976 paper-money era; blockchain structurally fills the gap of “rules and state independently recheckable”: cryptography and consensus substitute for part of reputation constraint; open-source code substitutes for opaque bank promises; competitive units shift from banknotes to verifiable rule suites—this has intellectual kinship with Hayek’s question.

On-chain deployability and auditable collateral state do not equal retail and tax having switched to on-chain units (on-chain real-payment metrics in Chapter 1, Section 8)²⁶. El Salvador’s Chivo wallet 2022 survey found only about 12% of respondents used it regularly²⁷. Hayekian competition on-chain first appears as changes in rule verifiability and participation structure. Terra/UST’s 2022 zeroing shows: even with transparent rules, parity promises can still trigger death spirals in confidence crises.

Section 8. Classical Presumptions and Protocol-Era Propositions

From Smith to Hayek, three centuries of monetary intellectual history hide four nearly default implicit presumptions across schools—the intellectual foundation of traditional monetary institutions. Each time the protocol era loosens one, a new proposition and a data-testable implication correspond; together the four form the book’s main argumentative line. The book’s claim can be stated in one sentence: money will not be abolished; the state’s monopoly of the mint prerogative will—when bookkeeping, transfer, and issuance rules can be publicly verified at low cost, discipline against overissue shifts from issuer reputation toward protocol-verifiable rules. This chapter’s four presumptions then supply implications that can be checked item by item against data.

First presumption: money must be guaranteed by a trusted subject. Classical tradition rests acceptance on state, central bank, or private-bank balance sheets. The protocol-era proposition: overissue discipline need no longer rest entirely on the issuer’s person; rules themselves must be independently checkable by third parties. What data can test: on monies with higher rule verifiability, transmission from the same issuer-reputation shock to purchasing power should be weaker than for like instruments with opaque rules relying on institutional backing; if that difference is unobserved, the claim of “constraint-carrier shift” should be narrowed.

Second presumption: modification of monetary rules must go through political or legal procedure. The gold standard was established by legislation and abolished by legislation; central-bank policy goals are set by political decision and then empowered by legal frameworks. Hayek hoped competitive pressure would replace legislative constraint, but competition itself still operated inside national legal frameworks. The protocol-era proposition: some rules can be encoded as machine states default-immune to unilateral tampering, separating rules from persons; revision may still occur, but via auditable procedures such as on-chain governance, not closed-room discretion. If in protocols whose parameter changes require on-chain disclosure and timelock activation, frequency and amplitude of sudden policy turns still show no systematic difference from committee discretion, then institutional advantages of “rules embedded in code” are overestimated—governance-capture risks discussed in Chapter 13, Section 4 must enter evaluation.

Third presumption: cross-border monetary circulation depends on interstate coordination. Classical monetary analysis takes nation-state borders as implicit boundaries; balance-of-payments adjustment, exchange-rate management, cross-border clearing-message networks, and RTGS coordination are all engineering patches that presuppose national monetary sovereignty. The protocol-era proposition: value transfer can cross jurisdictions; physical borders become optional constraints—interoperability standards (such as VTP value-transfer protocol, IBC cross-chain communication) are designed to lower marginal costs of multi-unit coexistence so competition need not wait for sovereign coordination. World Bank 2023 data show global remittance average cost about 6.2%, with Sub-Saharan African corridors still often above 8%²⁸; Chainalysis’s 2024 *Geography Report* shows

high-inflation economies such as Argentina and Turkey with significantly above-global-mean on-chain stablecoin receiving intensity²⁹. If on-chain adoption decouples from friction, then “protocols lower participation thresholds” must be re-explained with compliance interfaces, liquidity depth, and fiat on/off-ramps, not asserted a priori that monopoly is broken.

Fourth presumption: monetary stability is ultimately determined by the issuer’s incentive structure. Ricardo pinned hopes on metallic constraint; Keynes trusted institutional design; Friedman appealed to rules; Hayek bet on competition—four paths jointly assume that stability’s source is some constraint mechanism on human behavior. The protocol-era proposition: stability constraints can partly migrate to code’s deterministic execution and on-chain auditable state—collateral ratios, mint/redeem rules, supply caps need not depend entirely on “whether the issuer will self-discipline,” but partly on “whether rules are independently verified as executed.” PCIM (public overcollateralized issuance mechanism; Openverse instance VRC-10 + Bitgold) at the documentation layer adjusts collateral ratios by circulation-tier public votes, using redemption arbitrage and oracle circuit-breakers instead of MakerDAO-style liquidation/warning lines (upper tier near 161.8% collateral); this combination still awaits large-scale mainnet stress tests. Market repair speed after depeg or run should correlate positively with on-chain verifiability of collateral state, redemption queues (or liquidation queues in like CDP protocols), and supply curves; if repair speed correlates only with issuer PR or regulatory statements, then “verifiability” is insufficient as an independent discipline source—USDC’s brief 2023 depeg from Silicon Valley Bank exposure, with recovery speed related both to reserve disclosure and to federal intervention, shows that off-chain institutions still intervene above the “verifiable layer.”

Money endures; the mint prerogative can be dispersed; constraint shifts from reputation to verifiable rules—must be tested in high-friction scenes, not as an a priori conclusion. Classical economists asked the right questions: who issues money best? Rules or discretion? Competition or monopoly? Metallic anchor or managed float? Limited by tools of their age, they could not imagine protocol-era answers—especially silicon participants as economic agents needing no bank account. Actual evolution of monetary institutions is often driven more by war finance and election cycles than by academic optima; the gulf between theory and reality is a deep reason Hayek ultimately appealed to institutional competition rather than pure argument. Metallism, Keynesianism, monetarism, and Austrian competition theory, seemingly at odds, are all asking how to maintain balance between monetary convenience and power constraint.

注释与引用

1. Menger, 1892, "On the Origin of Money," §§1–2 (saleableness ranking; English Mises Institute PDF); in *Zeitschrift für die gesamte Staatswissenschaft*. https://cdn.mises.org/On%20the%20Origins%20of%20Money_5.pdf ↩ ↗²
2. Knapp, Georg Friedrich, *The State Theory of Money* (1905); Innes, A. Mitchell, "What is Money?" *Banking Law Journal*, May 1913, pp. 377–408 (state theory of money: tax acceptance and legal-tender commands draw the acceptance circle). ↩ ↗²
3. Goodhart, Charles A. E., "The two concepts of money: implications for the analysis of optimal currency areas." *Economic Journal* 108(447), 1998, pp. 377–390 (M-money vs C-money; cross-ref. Chapter 2, Section 5, Chapter 5, Section 2). <https://doi.org/10.1111/1468-0297.00291> ↩
4. Friedman, Milton, and Anna J. Schwartz, *A Monetary History of the United States, 1867–1960*. Princeton University Press, 1963, ch. 7 (1930–1933 money-supply contraction ~one-third). <https://press.princeton.edu/books/paperback/9780691003542/a-monetary-history-of-the-united-states-1867-1960> ↩
5. U.S. Bureau of Economic Analysis, Historical National Accounts; Bureau of Labor Statistics, Unemployment Rate 1929–1933 (~24.9% in 1933). <https://www.bea.gov/> ; <https://www.bls.gov/cps/> ↩ ↗²

6. Woodford (2003), *Interest and Prices*, chs. 6–7 (ELB and optimal inflation); Galí (2015), chs. 8, 15 (FIT); Christiano, Eichenbaum & Evans (2005), "Nominal Rigidities and the Dynamic Effects of a Shock to Monetary Policy," *Journal of Political Economy* 113(1), pp. 1–45; Smets & Wouters (2007), "Shocks and Frictions in US Business Cycles," *AER* 97(3), pp. 586–606. <https://doi.org/10.1086/426038> ; <https://doi.org/10.1257/aer.97.3.586> ↩ ↻ ↲
7. Holston, Kathryn, Thomas Laubach, and John C. Williams (2017), "Measuring the Natural Rate of Interest: International Trends and Determinants," *International Journal of Central Banking* 13(5), pp. 55–76 (U.S. r^* decline); BIS WP 1067 (2023), "Estimating the natural rate of interest in an open economy," §§2–4 (cross-country r^* and model sensitivity); Brunnermeier, Markus K., and Yann Koby (2019), "The Reversal Interest Rate," *AER* 109(8), pp. 2615–2647; Bindseil (2020), "Tiered CBDC and the Financial System," ECB WP 2351, §§3–5 (tiered CBDC and ELB transmission). <https://doi.org/10.1257/aer.20181007> ; <https://www.bis.org/publ/work1067.htm> ; <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf> ↩
8. Hayek, 1976, *The Denationalization of Money*, ch. 1 "A Realistic Proposal," revised-edition preface: advocate abolishing government's legal monopoly of money issue and opening private competition (PDF pp. 3–5, 83); Friedman, 1960, *A Program for Monetary Stability*, Fordham University Press, chs. 4–5 (k% rule constrains the existing central bank; does not advocate abolishing monopoly or opening private monetary competition). <https://fraser.stlouisfed.org/title/program-monetary-stability-3969> ; PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
9. Taylor (1993), "Discretion versus Policy Rules in Practice," *Carnegie-Rochester Conference Series on Public Policy* 39, pp. 195–214; Clarida, Galí & Gertler (1999), "The Science of Monetary Policy," *JEL* 37(4), pp. 1661–1707. [https://doi.org/10.1016/0167-2231\(93\)90009-L](https://doi.org/10.1016/0167-2231(93)90009-L) ; <https://doi.org/10.1257/jel.37.4.1661> ↩ ↻
10. Sargent & Wallace (1981), "Some Unpleasant Monetarist Arithmetic," *Minneapolis Fed Quarterly Review*, Fall 1981, pp. 1–17; Leeper (1991), "Equilibria under 'active' and 'passive' monetary and fiscal policies," *Journal of Monetary Economics* 27(1), pp. 129–147; Sargent (1982), "The Ends of Four Big Inflation," *Inflation: Causes and Effects*, pp. 41–98. <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ; [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ↩ ↻
11. Mises, 1912, *The Theory of Money and Credit*, Liberty Fund 1980 ed., pp. 264–266, 440–445: circulation-credit expansion triggers boom–liquidation cycles. English: <https://www.econlib.org/library/Mises/msT.html> ↩
12. Mises, 1912, *The Theory of Money and Credit*, ch. 8; Liberty Fund 1980 ed. pp. 111–123 (regression theorem: present prices must be traceable to commodity demand). <https://www.econlib.org/library/Mises/msT.html> ↩
13. Kiyotaki, Nobuhiro, and Randall Wright. "On Money as a Medium of Exchange." *Journal of Political Economy* 97(4), August 1989, pp. 927–954; Kiyotaki & Wright, "A Search-Theoretic Approach to Monetary Economics." *AER* 83(1), March 1993, pp. 63–77 (intrinsic/extrinsic saleableness; formal contrast with Mengerian emergence and Mises regression theorem). <https://doi.org/10.1086/261634> ; <https://doi.org/10.1257/aer.83.1.63> ; cross-ref. ch06 §4 ⁶. ↩
14. White, Lawrence H., "Competitive Payments Systems and the Unit of Account." *American Economic Review* 84(3), June 1994, pp. 699–712 (competitive issue and unit-of-account convergence); Selgin & White, "How Would the Invisible Hand Handle Money?" *Journal of Economic Literature* 32(4), 1994, pp. 1718–1749 (clearinghouses, option clauses, and the unit-of-account problem). <https://doi.org/10.1257/aer.84.3.699> ; <https://doi.org/10.1257/jel.32.4.1718> ↩
15. Selgin, George, "Synthetic Commodity Money." *Journal of Financial Stability* 17, 2015, pp. 92–99. <https://doi.org/10.1016/j.jfs.2015.01.002> ↩ ↻
16. Wei Dai (1998), "b-money" (distributed ledger + proof of work; credited in Satoshi Bitcoin white paper References); Nakamoto (2008), §§1–4 (timestamp server, PoW, longest chain); Narayanan et al. (2016), *Bitcoin and Cryptocurrency Technologies*, Princeton, Ch. 3–5 (textbook survey of consensus and mining economics). <https://www.weidai.com/bmoney.txt> ; <https://bitcoin.org/bitcoin.pdf> ; <https://bitcoinbook.cs.princeton.edu/> ↩
17. Szabo (2002), "Shelling Out: The Origins of Money" (collectibles cooperation and monetary origins); Szabo (2017), "Money, Blockchains, and Social Scalability" (social scalability: verifiable rules substitute for interpersonal trust costs). <https://nakamotoinstitute.org/shelling-out/> ; <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↩
18. Calomiris, Charles W., and Stephen H. Haber, *Fragile by Design: The Political Origins of Banking Crises and Scarce Credit*. Princeton University Press, 2014, ch. 2 (U.S. vs Scottish bank-charter political economy). ↩
19. Selgin, George, "The Legal Restrictions Theory of Money: A Reappraisal." *Cato Journal* 6(1), Spring/Summer 1986, pp. 479–497 (layered legal restrictions vs competitive failure; read with Calomiris & Haber 2014, Selgin 2010 on the 1865 federal

- tax). Cross-ref. Chapter 4, Section 2 ⁹, Chapter 5, Section 2 ². <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1986/5/cj6n1-4.pdf> ↩
20. Cross-reading: ch02 §5 ⁵ (Zimbabwe three readings) ↔ ch05 §2 ¹⁵²⁸ (Thiers + M/C-money) ↔ this chapter §7 ²¹²² (Hayek Gresham/Thiers boundary + Rolnick-Weber). Terminological discipline: Thiers and Gresham are two elimination directions under different institutional premises, not an "inversion" of the same law. ↩
21. Hayek, 1976, *The Denationalization of Money*, pp. 42–43 (ch. 6 "Gresham's Law"): "Gresham's law will apply only ... fixed rate of exchange enforced by Law"; under variable rates "good money drives out bad." Bresciani-Turroni, *The Economics of Inflation* (1937), ch. 4, p. 174 (Weimar: after official parity failed, paper marks discounted at market—Hayek cites this to show not a Gresham "inversion"). Jevons, *Money and the Mechanism of Exchange* (1875), pp. 64–65, 82 (Spencer private coinage forced 1:1 equivalence → still fixed-parity Gresham). PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ; Bresciani-Turroni: <https://www.econlib.org/library/Bresciani-Turroni/btEI.html> ↩ ↩² ↩³
22. Rolnick, Arthur J., and Warren E. Weber, "Gresham's Law or Gresham's Fallacy?" *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1986, pp. 17–30 (Minnesota free-banking period: when discounting allowed, direction aligns with Thiers; when parity forced, Gresham embeds); cross-ref. Chapter 5, Section 2 ²¹. <https://www.minneapolisfed.org/research/quarterly-review/greshams-law-or-greshams-fallacy> ↩ ↩²
23. Hayek, 1976, *The Denationalization of Money*, pp. 27–28: in the assay age ordinary people could not judge fineness; government mint marks were once reasonable warranty; today that original advantage no longer suffices to support monopoly. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
24. Bagehot, 1873, *Lombard Street*, chs. 2, 7 (lender of last resort). <https://www.gutenberg.org/ebooks/4359> ↩
25. Hayek, 1976, *The Denationalization of Money*, pp. 23, 131: money supply is a knowledge problem; "Good money can come only from self-interest, not from benevolence"—competition beats monopoly. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
26. McKinsey Global Institute / Artemis metrics: on-chain adjusted real payments ~0.02% order of magnitude of global payment flows (2024); consistent with Chapter 1, Section 8 footnote metrics, not nominal transfer totals. ↩
27. Inter-American Development Bank, "Survey of Chivo Wallet Users in El Salvador," 2022 (~12% regular Chivo use; ~70% still mainly cash). <https://www.iadb.org/> ↩
28. World Bank, *Remittance Prices Worldwide*, Q3 2023 (global average ~6.20%; SSA region ~8.17%). <https://remittanceprices.worldbank.org/> ↩ ↩²
29. Chainalysis, *2024 Geography of Cryptocurrency Report* (stablecoin receiving intensity in high-inflation economies such as Argentina and Turkey). <https://www.chainalysis.com/> ↩

Part III: National Banks and Monetary Authorities

§ 8 The Birth and Functions of Central Banks

The central bank is not a fact of nature—understanding how it emerged from goldsmith banking, war finance, and crisis response is the premise for assessing whether on-chain protocols can compete with it.

The central bank is the most core institutional node of the modern monetary system, yet also the presence most easily taken for granted. It both issues money and supervises banks; both executes monetary policy and maintains the payment system; both is the bankers' bank and the government's bank—its functions' complexity contrasts sharply with its seemingly austere institutional appearance. This chapter approaches from historical evolution, tracing how central banks gradually emerged from the original practices of goldsmiths and merchant bankers, and how under pressures of financial crisis, war finance, and globalization they gradually accumulated today's nearly ubiquitous institutional authority. To judge under what conditions blockchain protocols may challenge existing central-bank institutions, one must first see this evolution clearly—what is at stake is far more than one more option on the payment interface.

Section 1. Goldsmith Banking and Early Monetary Credit

The historical origins of central banking trace to an institutional innovation in seventeenth-century London goldsmithing. Gold holders, for safety, deposited coin in goldsmiths' vaults; goldsmiths issued receipts as deposit certificates. These receipts gradually circulated among merchants, replacing physical gold as means of payment—because circulating receipts was far more convenient than moving coin. The critical turn was goldsmiths' discovery that depositors usually did not all withdraw gold at once; the volume of receipts actually circulating could exceed gold reserves in the vault. They therefore began lending out excess “deposits,” earning interest, while maintaining partial reserves for everyday withdrawal demand. Fractional-reserve banking thus began.

This innovation both created a powerful engine of credit expansion and planted the seed of the financial system's inherent fragility. When depositors doubted a goldsmith's solvency and flocked to withdraw gold, even a fully sound goldsmith might be forced to close for insufficient reserves—a bank run. Contagion lies in this: a run need not wait for true insolvency; rumor and panic alone can plunge any institution relying on fractional reserves into crisis. That logic still holds today; only the protagonists have shifted from goldsmiths to commercial banks, and occasionally to crypto exchanges.

By the late seventeenth century several prosperous European commercial cities already had banks of a public character: the Bank of Amsterdam, founded 1609, supplied standardized deposit bookkeeping and settlement services, avoiding chaos from uneven coin circulating in the city; Sveriges Riksbank, founded 1668, is the world's oldest still-operating central bank. Their common features: public credit replacing private credit, unified ledgers replacing dispersed credit networks, supplying more reliable payment-clearing foundations for commerce. They were not the full form of a central bank, but already showed embryonic functions of a bankers' bank.

Section 2. The Bank of England: Prototype of the Modern Central Bank

The founding of the Bank of England in 1694 was a milestone in monetary institutional history. Its birth owed less to pure monetary theory than to William III's political need for war finance against France. A group of London merchants subscribed £1.2 million of public debt in exchange for a government charter: forming the Bank of England as a limited-liability bank that could issue notes of equal value and supply continuing finance to the government. The government got urgently needed war funds; the merchants obtained monopoly rights of note

issue—a mutually satisfying political bargain that inaugurated the lasting symbiotic relation between government and central bank.

The Bank of England's evolution over the following two centuries clearly displays the gradual accumulation of central-bank functions. In the early eighteenth century it was mainly a commercial bank that happened to hold the government account; by the late eighteenth century, as other banks began placing reserves at the Bank of England, the latter gradually became the "bankers' bank." During and after the Napoleonic Wars (1803–1815), note overissue brought inflationary pressure; in the crises of 1847, 1857, and 1866, issue constraints set by Peel's Act were also forced into suspension. In 1844, Peel's Act (the Bank Charter Act 1844) legislatively concentrated issue rights in the Bank of England; issue rights of other private banks in England were gradually frozen; Britain's monetary system for the first time achieved issue monopoly¹.

Yet the most definitional evolution came after the 1866 Overend–Gurney crisis. Britain's largest discount house failed through reckless management, triggering a liquidity panic in London markets. The Bank of England then announced it would not rescue; panic spread rapidly; many banks and firms failed. After the crisis, Walter Bagehot in *Lombard Street* (1873) proposed the theoretical program of the "lender of last resort": when a liquidity crisis threatens the entire financial system, the central bank has a duty to lend freely to banks that can offer good collateral, while charging a penalty high rate to deter moral hazard. What Bagehot stressed was systemic responsibility for maintaining stability of the whole monetary system, not generous rescue of individual banks. The Bank of England thence began to position itself as the financial system's stability anchor, no longer merely another commercial institution.

The Bank of England's evolutionary history reveals a recurring institutional logic: almost every expansion of central-bank power occurs after crises, not through rational institutional design in calm periods. Each crisis exposes a blank in the existing frame; each emergency fill leaves a permanent institutional trace; the next crisis extends further on already expanded functions. This crisis-driven gradual expansion of power keeps the central bank's boundaries always blurred—it is not a special-purpose agency with clear functions, but a complex grown organically through more than two centuries of crisis response. Only seeing this evolution clearly can one assess CBDC and on-chain protocols' place in the existing financial system: if new technology is to interface with the central-bank system, what it faces is never a static institutional blueprint but a continually evolving institution with fuzzy boundaries.

Section 3. Birth of the Federal Reserve: Political Compromise and Technical Authority

If the Bank of England's birth was the result of gradual evolution, the Federal Reserve's establishment was crisis-driven political engineering. Nineteenth-century U.S. banking was known for dispersion, fragility, and frequent crisis: the nation had no unified central bank (the First and Second Banks of the United States both closed under political pressure); money supply swung sharply with seasonal economic fluctuations; national financial panics erupted every few years. The Panic of 1907 was especially severe; had J.P. Morgan of Morgan not personally coordinated, summoning bankers to inject capital and rescue the market, the entire New York financial system might scarcely have survived. That the financial stability of the world's leading economy should depend on one private banker's personal authority had become politically unsustainable.

The Aldrich Commission's research and the later secret Jekyll Island meetings brought bankers, politicians, and economists together, spending years designing the Fed's institutional frame. The Federal Reserve Act of 1913 established a system intentionally designed to disperse power: twelve regional Reserve Banks across the country, with the Federal Reserve Board in Washington at the center (later the Federal Open Market Committee became the core policy body). The structure sought political balance among East–West Coast financial interests,

agricultural states' local interests, and the federal government, avoiding a repeat of the Second Bank's destruction by political force.

In its first decades the Fed's independence was extremely limited; monetary policy often served fiscal needs. During World War II the Fed was required to maintain low rates to facilitate government bond finance, in effect becoming an appendage of the Treasury. Only with the 1951 Fed-Treasury Accord did the Fed formally obtain independent operational authority over monetary policy, able to manage short-term rates unbound by fiscal will. That accord founded the institutional basis of the postwar independent-central-bank regime and became an important reference for the later global central-bank independence movement. From 1913 to 1951 the Fed took nearly forty years truly to obtain policy independence—itsself evidence that central-bank independence is not a natural endowment but must be continually fought for and institutionally designed.

Section 4. Lender of Last Resort: Bagehot's Principle and Its Contemporary Variants

The lender-of-last-resort (LOLR) function is one of the fundamental marks distinguishing central banks from ordinary commercial banks. The classic statement of Bagehot's principle: in a liquidity crisis the central bank should lend freely, but at a high rate, against good collateral (freely lend at a penalty rate against good collateral)². The inner logic: liquidity crisis and solvency crisis must be strictly distinguished. Liquidity crisis is temporary—only market panic makes assets temporarily unrealizable; solvency crisis is fundamental—insolvency. The central bank should rescue only the former, not the latter; otherwise public resources make good private decision failures and create severe moral hazard.

Bagehot's principle faces enormous practical challenge: when crisis breaks, liquidity difficulty and solvency crisis are often hard to distinguish in the moment. Bank asset quality needs time to assess, and time is the scarcest resource in crisis. In the 2008 financial crisis the Fed in extremely short time supplied hundreds of billions of dollars of emergency liquidity to multiple large financial institutions, some of whose true solvency was then impossible to judge. Critics held this violated Bagehot's principle, rescuing institutions that should not have been rescued; supporters held there was no choice—any hesitation would cause larger systemic collapse.

In the financial turmoil of the 2020 COVID pandemic, the Fed's response speed and scale far exceeded 2008—its balance sheet about \$4.2 trillion in March 2020, about \$7.0 trillion by June the same year, and a peak near \$8.9 trillion in 2022³. Simultaneously the Fed supplied liquidity backing to junk-bond, corporate-loan, and municipal-bond markets—ranges rare in Fed history—extending “lender of last resort” far beyond the traditional banking system. Bagehot's principle was stretched to a degree of boundary blur; constraints of “good collateral” and “penalty rates” were almost emptied of force. What this evolution means for the long-run incentive structure of central-bank institutions remains an open discussion.

Inside the blockchain ecosystem, mechanisms analogous to LOLR logic have also been discussed. The 2022 LUNA/UST collapse and FTX failure showed that when the on-chain ecosystem lacks a LOLR, the speed and destructiveness of confidence collapse can be extreme. Some protocol designers proposed on-chain “emergency liquidity mechanisms”—injecting funds in crisis from protocol treasuries with sufficient reserves to stop panic liquidation spirals—yet MakerDAO's “Black Thursday” post-mortem shows that even with a surplus buffer, oracle delay, liquidation auctions, and governance response can still lag the market². That path awaits mainnet stress events and courtroom tests, and should not leap from technical possibility directly to the institutional conclusion that “protocols have internalized LOLR.” How to supply emergency liquidity while avoiding expectations of “on-chain too big to fail” is an institutional difficulty the maturation of on-chain monetary protocols cannot bypass.

Section 5. Payment Clearing: The Invisible Monetary Infrastructure

In public cognition of central banks, monetary policy often takes center stage while payment-clearing systems are almost invisible. The latter is the true foundation of the monetary system's everyday operation. Only by clarifying the layered structure of modern payment systems can one assess what links CBDC and on-chain assets may alter.

Modern payment systems usually divide into three layers. At the bottom are central-bank reserves: commercial banks hold accounts at the central bank with reserves; final interbank clearing is completed by debiting and crediting these reserve accounts. This is the payment system's final-settlement layer, with the character of "ultimate money"—whatever happens to commercial banks, transfers between reserve accounts have no counterparty risk. The second layer is the commercial-bank account system: household and firm checking deposits and demand accounts are commercial-bank liabilities, ultimately backed by central-bank reserves. Retail payments—cards, transfers, checks—complete at this layer; commercial banks handle internal clearing after netting. The third layer is private payment infrastructure: payment networks, card schemes, clearinghouses—pipes connecting payment instruments to commercial-bank accounts.

This layered structure means that even a simple transfer between two banks may involve four to six institutions behind the scenes: paying bank, receiving bank, card scheme or payment network, possible intermediary banks, and final settlement through central-bank reserve accounts. Each link has fees, settlement cycles, and counterparty risk. Payment-system complexity is the sediment of history—each added intermediate layer often solved a then-specific technical or regulatory problem, but stacked they form today's forbidding architecture. That complexity itself is a barrier to market entry: institutions able to understand, access, and operate compliantly in this multi-layer system are few, and therefore capture considerable rents. Cross-border payments are more complex: correspondent banking requires a bank holding accounts in both countries as intermediary; remittances may pass three or four correspondents, take days, and stack fees. This system was an engineering optimum under twentieth-century technical conditions; public-chain transfers have shown lower marginal cost in some scenes, yet wholesale clearing, AML compliance, and the central-bank reserve layer remain dominated by permissioned systems—BIS 2023 reports' assessment of retail on-chain payment share shows that in most advanced economies volumes remain far smaller than card schemes and account systems⁴. Technical possibility is not monopoly loosening; one must test with observable metrics such as clearing share, remittance cost, and compliance-interface coverage, not preset outcomes from white-paper roadmaps.

Payment clearing's impact on financial inclusion is the most direct expression of this infrastructure's exclusivity. Becoming a participant in correspondent networks requires holding accounts in target countries, meeting strict compliance standards, and maintaining sufficient nostro balances. These thresholds rose sharply over the past decade with U.S. AML enforcement; many small banks and mid-sized developing-country banks were cut from correspondent relations by large international banks citing excessive risk cost—the so-called "de-risking" trend⁴. World Bank 2023 data show global remittance average cost about 6.2%, with Sub-Saharan African corridors still often above 8%⁵. On-chain stablecoins and Bitcoin's Lightning Network have shown technically feasible alternative paths in some high-friction corridors—phenomena of above-global-mean on-chain stablecoin receiving intensity in high-inflation edge economies. Read them as complementary tools and local realities, not as sufficient evidence that payment monopoly has collapsed.

CBDC discussion must be understood back within this layered structure, not as yet another "App payment." The 2020 joint report of the BIS and seven major central banks positions retail CBDC as a digital extension of cash—like reserves and paper notes a central-bank liability, but public-facing, programmable, and potentially

offline—not as replacing commercial-bank credit intermediation⁶. Bindseil’s latest ECB survey summarizes motives in three layers: when cash use shrinks, the public must still be able at face value to convert commercial-bank deposits into public money without counterparty risk, or the two-tier monetary system’s “1:1 promise” loses its everyday verification channel; if private stablecoins and large platforms become the default payment rail, they may spill from medium function into unit of account and erode monetary sovereignty; wholesale CBDC mainly upgrades the interbank final-settlement layer. Hayek advocated competing currencies, yet even in parallel-currency experience cited in Chapter 7 of *The Denationalization of Money*, the public monetary anchor remained the last reference for private-note redemption—today’s CBDC debate’s core disagreement is no longer “whether public money,” but in what architecture, with what limits, with what privacy boundaries public money exists in the digital age. For on-chain protocols this means CBDC may occupy the institutional home field at the payment-stack base and wholesale clearing layer, while leaving gaps in retail programmability and cross-border permissionless access—gap size depends on national design choices; technology itself does not predetermine outcomes.

Niepelt’s 2024 *Journal of Finance* calibration formalizes this layered problem: when banks have market power on the deposit side and liquidity transformation produces negative externalities, the optimal monetary architecture should minimize the social cost of liquidity supply; under most parameters CBDC supplies liquidity more efficiently than deposits, unless the central bank must refinance banks at high cost to offset deposit outflow—then CBDC’s optimal payment share must instead be compressed⁷. This dialogues with Bindseil’s policy orientation of deliberately making retail CBDC “payment-type” (non-interest-bearing, holding caps): academically CBDC can beat deposits; politically one must prevent it becoming a store-of-value asset competing with Treasuries. Keister and Monnet respond from another angle to the common worry that “CBDC worsens runs”: once depositors hold a CBDC option, banks in normal times reduce maturity mismatch, thus *ex ante* exposure to runs falls; meanwhile the speed of crisis-period flows into CBDC itself becomes an observable signal for supervisors, helping identify weak banks earlier—when well designed, CBDC may lower rather than raise financial fragility⁷. One should not therefrom predict national CBDCs’ inevitable success; one must see: unlike Hayek-era “parallel paper,” today’s CBDC design presupposes known disintermediation and run risks, using holding caps, waterfall mechanisms, and tiered remuneration as institutional hedges—if on-chain protocols compete at the retail layer, they will face this “public option with guardrails,” not naked central-bank liabilities.

Engineering constraints on interoperability are stated more concretely in the BIS 2021 supplement to seven central banks’ principles: retail CBDC must coexist with existing RTGS, card schemes, and account systems—identity, wallet, and ledger layers each interface, not overnight replace the wholesale clearing stack, or “front-end CBDC, back-end still via correspondents” breakpoints appear⁸. Wholesale CBDC mainly upgrades the final-settlement layer: Carapella and Fleischman (2020) in a Fed survey position it as payments innovation—digitizing central-bank reserves and introducing distributed ledgers, with far less political controversy than retail disintermediation, yet still needing coexistence with RTGS rather than overnight replacement⁹. Bindseil’s 2024 survey policy-izes this reality: intermediated architecture leaves customer relationships to banks and payment institutions, the central bank maintaining back-end liability registration; direct architecture opens accounts at the central bank, amplifying disintermediation and privacy controversy together. Brunnermeier, James, and Landau add from competitive structure: if large platforms bundle payments, data, and credit into closed-loop balances, erosion of bank liabilities has more than one CBDC channel—retail CBDC is here envisioned as a public option to maintain unit-of-account unity¹⁰.

Barrdear and Kumhof place the above institutional choices in a calibratable macro frame in BIS Working Paper 488 (2016): if retail CBDC raises the public’s convenience in holding “safe, highly liquid assets,”

aggregate welfare may rise—but bank-intermediation contraction lowers equilibrium credit and output unless the central bank recycles CBDC issuance proceeds into the banking system (e.g. swapping CBDC for Treasuries, then injecting liquidity into interbank markets)¹¹. This conclusion aligns with Niepelt’s 2024 calibration that “CBDC’s optimal payment share must differentiate from reserve rates”: the question is not whether CBDC can exist, but who, at what price, replenishes liquidity after it migrates from deposits. Bindseil’s deliberately making retail CBDC a non-interest-bearing, capped payment-type liability can be read as an institutional compromise with those macro externalities—sacrificing some potential welfare to keep bank balance sheets from being emptied overnight. The “unified ledger” vision in the BIS 2023 *Future Monetary System* report takes another path: wholesale CBDC, tokenized deposits, and on-chain assets settle atomically on the same programmable stack—not replacing banks with CBDC, but placing the final-settlement layer and composable contract layer side by side; if on-chain VRC-10-class public money is to interface with this stack, what it contests is interface eligibility for verifiable settlement finality, not the default retail-wallet option¹¹.

When Hayek discussed private-money circulation in Chapter 8 of *The Denationalization of Money*, he stressed that public acceptance still presupposes redemption into public money at face value—the nineteenth-century parallel-note redemption window was that everyday test. Today’s CBDC ambition is to make the test shift from queueing at branches to instant, programmable conversion inside wallets; if on-chain protocols are to coexist in the same jurisdiction, they must answer: when do users need central-bank liabilities, when verifiably collateralized protocol liabilities—the two held in parallel layers, each with its charge, not zero-sum replacement; competitive units move up from named banks to distinguishable protocol rule suites; division boundaries must be tested with penetration and compliance-interface data, not fixed a priori.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) coordinates global interbank messaging; it holds no funds and performs no settlement, only transmitting payment instructions, and with national RTGS forms the backbone of cross-border payments; its geopoliticalized uses appear in Chapter 11, Section 7.

Section 6. Financial Stability and Macroprudential Supervision

The 2008 financial crisis was another watershed in the evolutionary history of central-bank functions. The prior central-bank policy frame basically followed the lean logic of “inflation targeting”: keep inflation in the target band and leave the rest to markets—Fisher in *Stabilizing the Dollar* (1920) had already treated uncertain dollar purchasing power and unstable price levels as fundamental defects of the monetary system, advocating indexed adjustment toward predictable price stability¹². Financial stability was treated as the responsibility of financial supervision, independent of monetary policy. Crisis shattered that division of labor: systemic real-estate bubbles accumulated under calm inflation indicators; securitized-product risk contagion spread outside the supervisory frame; once the bubble burst, its shock to the real economy and monetary-policy goals was devastating. The central bank could not stand aside on financial stability. Friedman, from monetary-history research, further argued that monetary policy’s first duty is to prevent money itself from becoming a major source of economic disturbance; major contractions such as the Great Depression often accompanied central-bank policy mistakes or monetary disorder¹³.

Macroprudential policy is the institutional fruit of that reflection. Its core concern is systemic risk, not single-institution risk: banks may each operate normally, yet the whole system be collectively fragile through common exposures, procyclical behavior, and liquidity contagion. Macroprudential tools include: countercyclical capital buffers (requiring banks to accumulate extra capital in booms, releasable in crises), loan-to-value caps (limiting mortgage leverage), additional capital requirements for global systemically important banks (G-SIBs), and stress

tests. These tools adjust dynamically across phases of the financial cycle, aiming to smooth credit cycles rather than let them resonate with sentiment.

Systemic-risk forms in crypto assets both resemble and differ from traditional banking. On-chain protocols’ “composability” brings extremely strong inter-protocol correlation: a collateral protocol’s problem can rapidly transmit via staking relations to lending protocols relying on that collateral, then trigger cascading liquidations in stablecoin mechanisms using related tokens as reserves—the 2022 UST/LUNA collapse’s large-scale on-chain liquidations fully displayed such contagion’s speed and breadth. Yet crypto macroprudential management faces unique challenges: on-chain protocols have no administrative supervisor to enforce countercyclical capital requirements; dispersed governance-token holding makes collective coordination extremely difficult; ease of cross-chain asset transfer makes regulatory arbitrage easy. These challenges will sharpen further in scenes where CBDC and on-chain assets may deeply fuse; as white papers envision, robust mechanisms can be parameterized at the protocol layer or supplemented at the permissioned supervisory layer—whether either can replace traditional macroprudential tools, and which dominates, awaits mainnet scale and cross-border enforcement tests, and should not a priori assert that “regulatory intervention can be spared.”

Central-bank functional expansion in financial stability further intensifies role tension. On one hand, financial-stability functions require the central bank to hold broad information rights and intervention powers over financial institutions; on the other, exercising those powers often involves differential treatment of particular institutions and markets, with fuzzy boundaries and limited accountability. When the central bank is both monetary-policy maker, financial-stability gatekeeper, and de facto supervisor of some industries, the meaning of its “independence” becomes especially complex—independent of what, accountable to whom, who supervises the supervisor?

Section 7. Central-Bank Independence: Theoretical Ideal and Practical Compromise

The theoretical basis of independent central banks comes from deep insight into the time-inconsistency problem, formally modeled by economists Kydland and Prescott (later Nobel laureates) in 1977. Core logic: under electoral pressure governments always have motive to stimulate the economy and create jobs in the short run—even at long-run inflationary cost. Once the private sector understands that preference, it builds inflation expectations into wage and contract bargaining in advance; the result is rising inflation with no employment gain. Friedman in his 1968 AEA presidential address reached a similar conclusion by another path: there is “no permanent trade-off” between inflation and unemployment; temporary trade-offs come from unanticipated inflation rises, not inflation itself¹⁴—if the central bank tries to buy employment with inflation, public expectations adjust accordingly and the Phillips curve tends vertical in the long run. The solution is to delegate monetary policy to an independent institution unconstrained by short-run political pressure, whose mission is long-run price stability, not short-run employment stimulus. That argument supplied theoretical basis for the global central-bank independence movement and drove large-scale central-bank institutional reform from the 1990s through the 2000s.

Independent central banks’ empirical performance in the 1990s and 2000s was indeed impressive: most advanced economies achieved the “Great Moderation,” low inflation with low volatility. Yet after the 2008 crisis, political pressure on central-bank independence rose sharply. Post-crisis ultra-low rates and unconventional easing’s distributional effects (see Chapter 3, Section 2; Chapter 9, Section 4) still leave defense of “purely neutral monetary policy” unable to stand in political opinion: when policy tools intertwine with fiscal bond purchases and portfolio rebalancing, “independence” looks more like an operational firewall than a waiver of distributional effects. On the other hand, when fiscal expansion and monetary easing must coordinate against

crisis, the firewall between central bank and government has in fact been pierced; independence becomes a fact of technical operation rather than an institutional constraint.

Globally, substantive guarantees of central-bank independence vary enormously by country. Some central banks have mandatory statutory mandates and clear legal protection from political intervention; others are merely policy-executing arms of government departments, whose policy orientation can change with a change of leadership. Whatever the institutional design, when government's fiscal needs fundamentally conflict with the central bank's stability goals, history repeatedly proves that political force ultimately reasserts control of monetary policy through formal or informal channels. That observation does not deny central-bank institutions; it only signals their fragility—and thereby shows that protocol-layer rule constraints carry different institutional meaning. Central-bank independence and blockchain protocols' rule constraints in fact represent two different paths to the same problem: the former relies on institutional design and personnel selection to build a firewall against political intervention inside the political system; the latter relies on cryptography and distributed consensus to create technical obstacles to any single party overriding rules. Their reliability roots in entirely different trust foundations, each with comparative advantages and limits under different historical conditions.

Section 8. The International Monetary System and Central Banks' Supranational Role

In 2013 the Bank of Japan launched “quantitative and qualitative easing” (QQE); its balance sheet over a decade expanded from about ¥160 trillion to over ¥700 trillion, once exceeding 130% of GDP—far above the Fed's contemporaneous level¹⁵. The case shows: even with a statutory mission of price stability, under fiscal-financial pressure a central bank may long deviate from traditional balance-sheet scale. Abenomics in 2013 bundled monetary policy, fiscal stimulus, and structural reform; central-bank independence bore continuing strain in public and political interaction.

The UK Banking Act 1997 transferred the Bank of England's monetary-policy function to an independent Monetary Policy Committee (MPC), institutionalizing inflation targeting. That reform was a direct legislative product of Kydland–Prescott “time inconsistency” theory: stripping rate decisions from the finance minister's hands to reduce electoral-cycle distortion of monetary policy¹⁶. The New Keynesian tradition represented by Woodford and Galí then supplied a welfare case for an about-2% inflation target—under nominal rigidities moderately positive inflation buffers relative-price adjustment and lowers the probability of ELB constraint—making FIT one of the core clauses of the post-1971 fiat “monetary constitution”¹⁷. Bernanke et al. (1999) summarized multi-country inflation-targeting practice as institutionalized consensus: transparent communication + 2% anchor + independent operation¹⁸; Orphanides (2003) warned that even with Taylor-rule-style benchmarks, historical deviations recur—institutional design must be read with observable execution, not legal text alone¹⁸.

A single country's central-bank institutions are embedded in a broader international monetary system. The Bretton Woods system (1944–1971) was the most mature attempt yet at supranational monetary coordination: the dollar linked to gold, other major currencies to the dollar, forming a fixed-exchange-rate network, with the IMF coordinating national balance-of-payments imbalances. The system conferred on the Fed de facto global-central-bank status—foreign reserves denominated in dollars; U.S. monetary policy spilled over to other countries through global capital flows whether they wished it or not.

Bretton Woods' collapse (Nixon's 1971 announcement of dollar–gold decoupling) did not end dollar global dominance; it continued and strengthened in the form of the “petrodollar system.” Global commodities price in dollars; countries accumulate dollar reserves; Fed rate decisions in substance shape the global credit cycle. Such “spillover effects” are especially strong in emerging markets: Fed hiking cycles often trigger emerging-market capital outflow, exchange-rate depreciation, and domestic credit contraction, while the Fed's policy targets are

U.S. domestic inflation and employment, with no duty to heed impact on other countries. Former RBI governor Raghuram Rajan put it bluntly: when the Fed turns, emerging markets must “fend for themselves.”

The Bank for International Settlements (BIS) is central banks’ “central bank,” supplying international settlement services and coordinating formulation of global financial regulatory standards. The Basel Accords (I, II, III) established global minimum capital-adequacy standards for commercial banks, seeking through a unified supervisory frame to reduce regulatory arbitrage and cross-border contagion of systemic risk. After the 2008 crisis, Basel III sharply raised capital requirements, introduced the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), and systematized macroprudential logic into a globally common rule frame.

This international monetary coordination system forms an institutional contrast with blockchain paths that, as white papers envision, establish value-transfer standards outside sovereign authorization—the former depends on coordinated authorization by national central banks and international organizations; the latter, if realized, tries to replace some clearing intermediaries with verifiable protocols. The two paths may meet or friction at cross-border payment standardization, stablecoin interfaces, tokenized RWA atomic settlement, and elsewhere; which path dominates in which scenes must be tested with observable metrics (clearing share, remittance cost, reserve-currency structure), not preset by technical narrative. Central banks in this landscape will simultaneously play multiple roles—competitor, supervisor, and potential partner—role combinations varying by country; possibility is not institutional reality.

注释与引用

1. Bank Charter Act 1844: separates Bank of England Issue and Banking Departments, gradually freezes other English banks' issue rights; constraints suspended in 1847, 1857, 1866 crises. Fetter, Frank W. (1965), *Development of British Monetary Orthodoxy, 1797–1875*, Harvard University Press, chs. 7–9 (Peel's Act and Issue Department institutional history). Bank of England charter: 1694 Tonnage Act authorized £1.2 million subscription. <https://www.bankofengland.co.uk/about/history> ↩
2. Bagehot (1873), *Lombard Street*, ch. 2 ("A More Exact Knowledge of Lenders' Last Resort"), ch. 7 (in crisis must "lend freely ... at a rate high enough to deter borrowers who do not really need it"): good collateral + penalty high rate, distinguishing liquidity from solvency crisis. <https://www.gutenberg.org/ebooks/4359> ; MakerDAO Black Thursday Post Mortem (2020-03-12) as contrast case of protocol-layer lack of LOLR; see bibliography.md. ↩ ↩²
3. Federal Reserve H.4.1 *Factors Affecting Reserve Balances* (FRED series WALCL): 2020-03-04 ~\$4.29T → 2020-06-10 ~\$7.17T → 2022-04-13 peak ~\$8.96T (billions of dollars). <https://fred.stlouisfed.org/series/WALCL> ↩
4. BIS (2023), *The Future Monetary System* (Annual Economic Report, Chapter III), §III.B: permissioned clearing layer still dominates wholesale and retail payments; de-risking's contraction effect on correspondent networks. <https://www.bis.org/publ/arpdf/ar2023e3.htm> ↩ ↩²
5. World Bank (2023), *Remittance Prices Worldwide* Q3 2023: global average ~6.2%; many Sub-Saharan African corridors >8%. <https://remittanceprices.worldbank.org/> ; Chainalysis 2024 *Geography of Cryptocurrency Report* stablecoin receiving intensity in high-inflation economies: see Chapter 7, Section 8 testable implications. ↩
6. BIS and seven central banks (2020), *Central Bank Digital Currencies: Foundational Principles and Core Features*, §§1–3: CBDC as digital form of cash, without harming financial stability and monetary policy; Bindseil (2024), ECB Occasional Paper 322, §§2–4 (motives: public monetary anchor, monetary sovereignty, wholesale clearing): <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op322~5822218919.en.pdf> ↩
7. Niepelt (2024), "Money and Banking with Reserves and CBDC," *Journal of Finance* 79(4), pp. 2505–2552 (optimal architecture; CBDC and reserve rates should differentiate); Keister & Monnet (2022), "Central Bank Digital Currency: Stability and Information," *Journal of Economic Dynamics and Control* 142, 104501 (OFR WP 22-04, §§1–2, §3.3): CBDC

reduces maturity mismatch and information effects. <https://www.niepelt.ch/files/jf2024.pre.pdf> ; https://www.financialresearch.gov/working-papers/files/OFRwp-22-04_central-bank-digital-currency.pdf ↩ ↩²

8. Group of Central Banks and BIS (2021), *Central bank digital currencies: system design and interoperability*, §§2–3 (three-layer architecture: identity/wallet/ledger; coexistence with existing systems): <https://www.bis.org/publ/othp38.htm> ↩
9. Carapella, William, and Leland D. Fleischman. "Wholesale central bank digital currency: payments innovation, and the case for implementation." *FEDS Notes*, Board of Governors of the Federal Reserve System, September 25, 2020 (wholesale CBDC upgrades final-settlement layer, coexistence with RTGS); BIS Committee on Payments and Market Infrastructures (2021), "Central bank digital currencies: financial stability implications," *BIS Papers* No. 113, §§II–III (wholesale vs retail CBDC financial-stability division). <https://www.federalreserve.gov/econres/notes/feds-notes/wholesale-central-bank-digital-currency-payments-innovation-and-the-case-for-implementation-20200925.html> ; <https://www.bis.org/publ/bppdf/bispap113.htm> ↩
10. Brunnermeier, James & Landau (2019), "The digitalization of money," BIS WP 941, §5.2 (platform closed-loop money vs bank liabilities vs public CBDC option): <https://www.bis.org/publ/work941.pdf> ↩
11. Barrdear, John, and Michael Kumhof. "The macroeconomics of central bank issued digital currencies." *BIS Working Paper* 488, July 2016, pp. 5–12 (CBDC convenience gains vs bank-intermediation contraction; recycling conditions); BIS (2023), *The Future Monetary System* (Annual Economic Report, Chapter III), §III.C (unified ledger: wholesale CBDC + tokenized deposits + on-chain assets composable settlement). <https://www.bis.org/publ/work488.htm> ; <https://www.bis.org/publ/arpdf/ar2023e3.htm> ↩ ↩²
12. Fisher, 1920, *Stabilizing the Dollar*, preface: "The fundamental fact on which the proposal of this book is based is that the purchasing power of the dollar is uncertain and variable, that is, that the price level is unstable." PDF: https://fraser.stlouisfed.org/files/docs/publications/books/stabilizing_fisher.pdf ↩
13. Friedman, 1968, "The Role of Monetary Policy," *American Economic Review* 58(1), pp. 12–13: "the first and most important lesson ... is that monetary policy can prevent money itself from being a major source of economic disturbance"; and noting the Great Contraction "might not have occurred at all ... if the monetary authority had avoided mistakes." PDF: https://www.cooperative-individualism.org/friedman-milton_the-role-of-monetary-policy-1968-mar.pdf ↩
14. Friedman, 1968, "The Role of Monetary Policy," p. 11: "there is always a temporary trade-off between inflation and unemployment; there is no permanent trade-off. The temporary trade-off comes not from inflation per se, but from unanticipated inflation, which generally means, from a rising rate of inflation." PDF: https://www.cooperative-individualism.org/friedman-milton_the-role-of-monetary-policy-1968-mar.pdf ↩
15. Bank of Japan (BOJ) balance sheet: ~¥164T at QQE launch April 2013 → ~¥733T in 2023; peak share of nominal GDP ~132% (2018–2019, BOJ *Balance Sheet* and Cabinet Office GDP series). <https://www.boj.or.jp/en/statistics/boj/other/acmai/index.htm> ↩
16. Kydland & Prescott (1977), "Rules Rather than Discretion," *Journal of Political Economy* 85(3), pp. 473–491: time inconsistency of optimal plans—period-by-period revision leads to departure from ex ante commitment; inflation targeting and central-bank independence as institutional responses. <https://doi.org/10.1086/260580> ↩
17. Woodford (2003), *Interest and Prices*, ch. 6 (pp. 235–280, optimal inflation under nominal rigidities), ch. 7 (pp. 281–330, ELB); Galí (2015), *Monetary Policy, Inflation, and the Business Cycle*, 2nd ed., ch. 8 (pp. 145–180, optimal monetary policy), ch. 15 (pp. 320–340, FIT). See Chapter 3, Section 3; Chapter 24, Section 2. ↩
18. Walsh (2017), *Monetary Theory and Policy*, 4th ed., MIT Press, chs. 8–11 (New Keynesian baseline, Taylor rule, and ELB textbook pages); Bernanke et al. (1999), *Inflation Targeting*, chs. 1–2 (pp. 1–45, institutionalizing inflation targeting and expectation anchoring); Orphanides (2003), "The Quest for Prosperity Without Inflation," *JME* 50(3), pp. 715–730 (historical Taylor-rule deviations). Princeton 1999 ed.; [https://doi.org/10.1016/S0304-3932\(03\)00028-7](https://doi.org/10.1016/S0304-3932(03)00028-7) ↩ ↩²

§ 9 Monetary Policy Tools and Transmission

With the central bank established, how monetary policy transmits to the real economy is the mechanism this chapter unpacks.

Monetary policy is the central bank's core means of steering the economy, and among the most watched and contested fields in modern macroeconomics. To the general public it is often reduced to a single phrase—"cut rates / raise rates"—as if the central bank could dial the economy's temperature with one knob. Reality is far more complex: from the policy signal to corporate loan rates, from ample liquidity to household spending decisions, several coupled transmission chains intervene, each of which can break or distort under market expectations, confidence shocks, or institutional frictions. This chapter surveys the main monetary-policy tools and traces their transmission paths and failure boundaries—equipment for dismantling the mechanisms of the traditional financial system, and a yardstick for what on-chain protocols can and cannot substitute in the function of economic stabilization.

Section 1. The Policy Rate: Monetary Policy's Core Lever

From March 2022 to July 2023, the Federal Reserve raised the federal funds target from near zero in successive steps to 5.25%–5.50%—one of the sharpest tightening cycles since the 1980s¹. Over the same period, U.S. 30-year mortgage rates briefly broke above 7%, and the commercial-real-estate refinancing window narrowed abruptly—transmission of the policy rate into the real economy showed almost in real time in housing and credit-sensitive sectors. The People's Bank of China relies more on the required reserve ratio and the Medium-term Lending Facility (MLF) to guide banking-system liquidity: in 2024 it cut the reserve requirement ratio several times by a cumulative roughly 1 percentage point, releasing more than RMB 1 trillion in long-term funds—illustrating differentiated tool mixes under a bank-dominated financing system¹.

In most advanced economies, the most direct operating tool of monetary policy is the **policy rate**—the very short-term (usually overnight) borrowing rate set by the central bank. The Fed's federal funds target, the ECB's main refinancing operations rate, and the PBOC's open-market operation rates are typical instances. The central bank does not directly control long-term rates or loan rates, but by influencing the short-term funding cost of the financial system it affects the whole yield curve and broader credit conditions.

How does a policy-rate change affect the real economy? Textbooks usually list four transmission channels. **Intertemporal substitution**: higher rates lower the present value of future consumption, so households tend to save more and borrow less for consumption. **Cost-of-investment channel**: higher funding costs postpone or cancel projects whose marginal return falls below the financing cost. **Asset-price channel**: a lower discount rate lifts valuations of equities, real estate, and similar assets; wealth effects raise spending. **Exchange-rate channel**: higher rates attract foreign capital inflows, appreciate the domestic currency, make imports relatively cheaper and exports less competitive, and adjust the trade balance accordingly.

Setting the policy rate depends, technically, on estimates of the so-called "natural rate" (r^*)—the equilibrium real rate when output equals potential and inflation is at target. When the policy rate is above the natural rate, policy is contractionary; below it, expansionary. Yet the natural rate is not directly observable; it can only be inferred from models, and different models yield widely different estimates that evolve with economic structure. Holston, Laubach, and Williams (2017) estimate that the U.S. real natural rate r^* fell from about 3%–4% in the 1980s to near zero or slightly negative in the 2010s; a 2023 BIS working paper surveying major advanced economies finds a general decline in r^* and stresses high sensitivity to model specification—the r^* range for the

same country across periods can differ by more than 1 percentage point². In his 1968 presidential address, Friedman emphasized that the monetary authority can control nominal magnitudes and their rates of change, but “cannot use its control over nominal quantities to peg a real quantity”—the real interest rate, the unemployment rate, real national income, and so on³. Since the 2010s, the decline in r^* (possibly linked to aging, a global savings glut, and slower productivity growth) means that the nominal rate corresponding to neutral policy sits far below the 1980–2000 historical average. This “low natural-rate environment” is the key background for why global central banks kept rates near zero for so long after 2008, and why the rapid hiking after 2022 triggered sharp asset-price revaluations—what is observable is the policy-rate path and asset repricing; r^* itself remains a model inference and should not be treated as a precise operational target.

The effectiveness of rate policy depends on the depth of the financial system and the efficiency of transmission. In economies with deep markets where firms finance mainly through bonds and equities, policy-rate changes are reflected almost immediately across the credit market; in bank-dominated systems with sticky rate pass-through, the real effect of policy-rate adjustments may be heavily discounted. More fundamentally: the interest rate is both a monetary-policy tool and a price signal for intertemporal resource allocation; when the central bank actively pushes rates down or up, it inevitably interferes with the market’s informational function—the starting point of the Austrian business-cycle critique, and not without force.

On-chain lending-pool rates are set by contracts and the supply and demand for funds, eliminating discretionary control of the equilibrium rate by a single institution—but technical feasibility does not mean distortion has already been eliminated in practice: governance-parameter changes, oracle pricing, liquidity-mining subsidies, and MEV front-running can all pull observed rates away from a “pure supply–demand equilibrium”; in 2020–2021, DeFi lending rates under liquidity incentives long sat below the unsubsidized equilibrium, and only repriced after subsidies faded⁴. Thus “no central-bank discretion on-chain” at most yields an auditable constraint carrier; it does not a priori yield no systematic malinvestment. Countercyclical liquidity injection, a lender of last resort, and forward guidance under the ELB are, under current open-protocol architectures, not closed even on the *whitepaper*’s own terms, and must be compared separately with the macro-stabilizer functions of sovereign monetary systems—possibility must not be substituted for actuality.

Section 2. Open Market Operations and Base-Money Management

Open market operations (OMO) are the main technical means of day-to-day monetary-policy implementation. By buying or selling government bonds (or other eligible assets) in the secondary market, the central bank directly affects commercial banks’ reserve balances at the central bank, and thereby short-term funding supply and demand in the interbank market, guiding overnight rates toward the policy target.

When the central bank buys bonds, it injects equivalent funds into the selling bank’s reserve account; interbank funding supply rises and overnight rates fall. When it sells bonds, it drains reserves, tightens liquidity, and rates rise. The elegance of the mechanism is that the central bank does not lend directly to market participants; it controls the price of funds indirectly by adjusting the aggregate liquidity of the banking system.

The routine form of OMO is usually short-term operations with repurchase agreements (repo): the central bank provides overnight or seven-day funding against government bonds as collateral, automatically recalled at maturity. Liquidity injection thus has an automatic expiry property, avoiding permanent expansion of base money, and allowing fine management of reserve supply. Conventional OMO is highly effective for keeping the policy rate stable within its target corridor day to day, but its boundary is the short end of the curve; it cannot directly control ten-year Treasury yields, nor directly extend credit to particular entities—those tasks require other, more aggressive tools.

An important implicit premise behind OMO is that the government bond market is deep and liquid enough to serve as a reliable transmission medium for monetary operations. That premise usually holds in advanced economies, but not necessarily in emerging markets or small open economies. When the bond market is illiquid, the central bank's own buys and sells distort prices, OMO effectiveness collapses, and maintaining the policy-rate target becomes unusually difficult.

Section 3. Reserve Requirements and the Money Multiplier

The reserve requirement ratio is the institutional arrangement under which the central bank requires commercial banks to hold liquid reserves at the central bank equal to a stated share of deposit balances. Its historical function was originally to prevent runs—ensuring banks always had enough cash to meet withdrawals; after the twentieth century, the ratio gradually became a monetary-policy tool, adjusting the statutory ratio to influence the banking system's capacity to create credit.

The textbook “money multiplier” story is widely told: if the reserve ratio is 10%, one unit of base money can in theory support ten units of deposit money. Banks take deposits, keep 10% as reserves, lend the remaining 90%; loans flow into other banks as new deposits, and the cycle multiplies. The policy implication looks tidy: cut the reserve ratio, the multiplier expands, money supply inflates; raise it, the multiplier contracts, money supply tightens.

In reality money creation is far more complex. The Bank of England's 2014 *Quarterly Bulletin* article “Money creation in the modern economy” stated plainly that the multiplier model is a severe simplification of the actual process—commercial banks lend first and replenish reserves later: when a bank judges a loan profitable and risks manageable, it first credits the borrower's account and simultaneously creates a deposit on the liability side, rather than waiting for reserves and then multiplying; if reserves later prove insufficient, it borrows in the money market or seeks central-bank liquidity support⁵. Fisher's 1911 *The Purchasing Power of Money* already brought bank check deposits into the analysis of the circulating medium, linking money stock, deposits, velocity, and the price level in the equation of exchange $MV + M'V' = PT$ as a testable quantity relation⁶. In a liquidity-abundant environment, reserve constraints bind credit decisions only weakly; the real constraints are capital adequacy, loan demand, and banks' judgment of credit risk.

Accordingly, many advanced-economy central banks (the Fed since 2020, the ECB, and others) have abolished statutory reserve requirements, controlling overnight rates instead through an interest-rate corridor—a floor on the deposit rate and a ceiling on the lending rate at the central bank. The PBOC still retains the reserve ratio as a macro-control tool, mainly to lock up liquidity and coordinate exchange-rate management and credit pacing, not to control aggregate money supply through the multiplier mechanism.

If retail CBDC allows the public to hold central-bank liabilities directly, the policy implications of the above narrative must be reassessed: deposits are not only products of bank balance sheets, but also liquid claims that can be migrated at a click—the Bank of England's 2014 bulletin already made clear that “loans create deposits,” but did not assume depositors could move claims back to the central-bank end in seconds⁵. Brunnermeier and Niepelt's equivalence theorem supplies a benchmark for comparison: under particular fiscal–central-bank coordination and asset structures, issuing CBDC while adjusting reserves and Treasury holdings in theory need not change the monetary-policy stance—but the conclusion depends on deposit-outflow frictions being high enough and adjustment fast enough⁷. Niepelt's 2024 calibration shows that when CBDC's optimal share in payments rises, the CBDC rate should differentiate from the reserve rate; otherwise the social cost of liquidity provision is shifted onto bank refinancing channels—base-money management moves from “a single reserve price” to “spread management across two tiers of risk-free liabilities”⁸. Chiu, Davoodalhosseini, Jiang, and Zhu in

the *Journal of Political Economy* (2023) place the same question in a credit-creation setting: even at low adoption, CBDC can serve as an outside option in the deposit market, constraining banks' pricing power on the deposit side; if CBDC and bank deposits are near-perfect substitutes and the central bank does not recycle CBDC liabilities back into the banking system, the "loans create deposits" chain may be cut at the CBDC end—unless the central bank repoes bank assets against CBDC holdings or reinjects reserves into the interbank market⁹. Andolfatto's 2021 St. Louis Fed survey gives the mirror conclusion: CBDC need not be a zero-sum threat to banks—if CBDC pays no interest, holdings are capped, and the central bank redistributes incremental liabilities to banks as wholesale funding, private intermediation can maintain or even expand credit supply; the threat comes from interest-bearing, uncapped CBDC design, not from the technical form of CBDC itself⁹. For on-chain protocols, this means that after CBDC lands, the spread structure between "no central-bank discretion" on-chain rates and sovereign fiat rates may grow more complex, not simpler—the sovereign layer adds a policy variable of "public-liability recycling," while on-chain pool rates are still set by collateral and supply-demand; the arbitrage boundary between them must be tested with corridor data.

Section 4. Quantitative Easing: Logic and Practice of Unconventional Tools

The 2008 financial crisis pushed major advanced central banks to the zero lower bound on policy rates; traditional price tools were exhausted, and the Fed, Bank of England, Bank of Japan, and ECB successively activated quantitative easing (QE). Operational detail, purchase scale, and distributional consequences appear in Chapter 3, Section 2¹⁰; what follows is only the toolkit's placement and exit lessons.

The divide between QE and conventional OMO is the target maturity: the latter maintains the short-end policy rate; the former buys large volumes of medium- and long-term Treasuries (and MBS, corporate bonds, etc.) in the secondary market, compressing long-end yields and stimulating aggregate demand through portfolio rebalancing, signaling, and exchange-rate channels. Portfolio rebalancing means that after the central bank buys bonds, sellers (mostly institutional investors) hold cash and reallocate into corporate bonds, equities, and foreign assets; the signaling channel conveys a commitment to prolonged ease; the exchange-rate channel is especially sensitive in small open economies. Reviewing three rounds of QE's contribution to long rates and employment, Bernanke (2015) stressed effects that are lagged and capped, and intertwined with fiscal policy, regulation, and bank capital—one should not equate the single variable "purchase scale" with "strength of real recovery"¹⁰.

Systemic risks of QE exit were stress-tested in 2022–2023. From March 2022 to July 2023 the Fed raised the federal funds target from 0%–0.25% to 5.25%–5.50% and simultaneously ran quantitative tightening (QT); over the same period U.S. 30-year mortgage rates briefly exceeded 7%, and global risk assets sold off. Silicon Valley Bank (SVB) failed in March 2023: by end-2022 it held about \$91 billion of available-for-sale (AFS) Treasuries and MBS, with unrealized losses on the order of \$15 billion under rapid rate hikes, triggering a run—the FDIC took over¹¹. Testable lesson: ultra-easy periods of central-bank bond buying change financial institutions' duration structure and interest-rate risk exposure; exit itself can trigger procyclical credit contraction. Any stability mechanism that couples protocol issuance rules deeply to market rates must pre-specify interest-rate-reversal stress tests rather than assume low rates forever—PCIM redemption runs and MEV front-running are listed as scenarios in Chapter 14, Section 9, not as closed whitepaper conclusions.

Section 5. Multiple Channels of Monetary-Policy Transmission

From the central bank's rate decision to final effects on inflation and output, monetary policy does not travel a single channel but several intertwined paths, each with lags and intensities that vary by economic structure. Only by separating the channels can one see when monetary policy is precise and when it fails.

The interest-rate channel is the most direct: policy-rate changes affect the funding cost of firm investment and household consumption through bank loan rates and bond yields, and thereby aggregate demand. This channel is most efficient in economies with deep markets and flexible rate pass-through, and heavily discounted where rates are administered or the policy rate is detached from loan rates.

The credit channel stresses the active role of bank credit supply. Bernanke and Gertler (1995) formalized the “financial accelerator”: asset prices fall → collateral shrinks → banks tighten credit → investment falls → asset prices fall further, a self-reinforcing spiral¹². In the 2008 crisis, the Fed’s Senior Loan Officer Opinion Survey (SLOOS) showed large banks continuously tightening C&I loan standards from 2007Q3 through 2009Q1; even with the federal funds rate near zero, easy price tools and contracting credit supply can coexist—SLOOS data are thus verifiable evidence of the “pushing on a string” dilemma¹². Gilchrist and Zakrajšek’s (2012) excess bond premium further shows that the “pure financial friction” component of corporate spreads, beyond default expectations, is significantly associated with subsequent output declines—the credit channel is not banking rhetoric but a measurable macro variable.

The exchange-rate channel matters especially for small open economies: higher rates attract capital inflows, appreciate the currency, lower import prices and directly curb inflation; export prices rise, competitiveness falls, and the current account contracts. In highly trade-dependent economies, the exchange-rate channel is often the fastest path from monetary policy to inflation.

The expectations channel has grown ever more central in modern frameworks: expectations of future inflation themselves shape current wage bargaining and pricing, and thus become a leading determinant of current inflation. Friedman noted that the temporary inflation–unemployment trade-off comes from “unanticipated inflation,” which generally means a rising rate of inflation; once expectations are anchored, trading inflation for employment is ineffective in the long run¹³. If the central bank has strong credibility, merely announcing an inflation target can anchor expectations and greatly reduce the size of actual rate adjustments needed to hit the target¹⁴. Taylor’s (1993) Taylor rule operationalizes this logic as a systematic response to inflation and output gaps, becoming the empirical benchmark for the New Keynesian reaction function summarized by Clarida–Gali–Gertler¹⁵. Conversely, once inflation expectations de-anchor, dragging them back often costs large output and employment losses—Sargent (1999) casts Volcker’s 1979–1982 tightening as a classic case of rebuilding the inflation anchor under rational expectations¹⁶; Sargent’s (1982) historical study of the ends of four big inflations shows that anchor reconstruction often must proceed alongside fiscal reform, not central-bank verbal commitment alone¹⁵.

The relative importance of these four channels differs sharply across economies. In advanced economies with deep markets and freely floating rates, the interest-rate and expectations channels dominate; in bank-dominated developing economies, the credit channel matters more but often with low pass-through efficiency; in highly outward-oriented small open economies, the exchange-rate channel’s effect on inflation may exceed the others, so that monetary policy’s main task becomes exchange-rate management rather than domestic demand management. Such structural differences mean there is no universally optimal monetary-policy framework; each economy must design a tool mix suited to its own transmission mechanisms given its financial structure and trade openness. If on-chain protocols enter real-economy pricing and credit scenes, they must, even on whitepaper terms, face the same channel diversity—but current open protocols mainly cover collateralized lending and stable settlement and do not yet supply testable tools for countercyclical credit expansion and expectation anchoring; possibility (rules can be coded) ≠ actuality (macro transmission has already replaced the central bank)—compare with observable indicators at the margin, rather than presupposing wholesale substitution.

If retail CBDC scales, it will layer an still-untested transmission variable atop the channels above. Brunnermeier and Niepelt (2019) showed that under particular fiscal–central-bank coordination and asset structures, introducing CBDC can be equivalent to “central-bank liabilities to the public plus corresponding adjustments to the banking system,” and in theory need not change the monetary-policy stance—but the conclusion rests strictly on assumptions of no financial frictions and no deposit outflows⁷. Leeper (1991) reminds us that the fiscal–monetary institutional mix determines the final equilibrium—under “active fiscal, passive monetary” regimes, public-debt expansion is more likely to be validated by inflation, in the same direction as Sargent–Wallace (1981) arithmetical logic¹⁵. Once the public in a crisis converts bank deposits into CBDC (central-bank direct liabilities with no counterparty risk), credit-channel and bank-funding-cost transmission may diverge from inherited models; Bindseil therefore distinguishes “payment CBDC” (non-interest-bearing, with holding caps—e.g. the waterfall in digital-euro legislative drafts) from “investment CBDC” (interest-bearing, possibly strengthening pass-through of the policy rate to bank liabilities, but also hardening the zero lower bound). Bindseil’s 2020 tiered CBDC further operationalizes the distinction: balances for everyday payments at zero or very low rates, holdings above a threshold at a lower (even negative) CBDC rate, so that CBDC is inferior to bank deposits at the margin and disintermediation motives stay within “payment need” rather than “store-of-value arbitrage”—consistent with Agur et al.’s IMF working-paper numerical results on the CBDC rate–holding-cap–bank-disintermediation trilemma¹⁷. Brunnermeier and Koby’s (2019) “reversal rate” presses from the transmission side: if CBDC drains deposits and banks cannot fully pass negative policy rates through to retail depositors, net interest margins compress so that below a threshold banks reduce lending—further cuts tighten credit; tiered CBDC makes public liabilities inferior to deposits at the margin and can delay that constraint, but cannot erase the structural tension between the ELB and a clogged credit channel⁹. ECB assessments by Assenmacher and others of the digital euro hold that under a per-person holding cap of about €3,000 and non-interest-bearing design, disintermediation and disturbance to policy-rate transmission “may be limited”—Meller and Soons’s simulation of more than 2,000 euro-area banks further suggests that a €3,000 per-person cap may effectively contain liquidity-risk transmission even in pessimistic scenarios¹⁷. Nigeria’s eNaira low adoption shows that intent and outcome may still be separated by a network-effects gulf. Niepelt’s 2024 calibration warns that if CBDC’s optimal share in payments is higher than deposits, the central bank must set a CBDC rate differentiated from reserves, or shift the social cost of liquidity provision onto bank refinancing—tension with Bindseil’s conservative “payment-type, non-interest-bearing” design, and a theoretical frontier of monetary transmission that is not yet closed¹⁷.

The BIS Committee on Payments and Market Infrastructures’ 2022 report on stablecoins places the same tension back in an international competition frame: if global stablecoins form network effects in cross-border retail, they will force countries to accelerate CBDC deployment—not because on-chain assets are “better,” but because private digital dollars embedded in the payment stack may pull the unit of account and clearing outside domestic supervisory sight¹⁸. The platform closed-loop money of Brunnermeier, James, and Landau forms a triangle with stablecoins and CBDC: in-platform balances erode bank liabilities; stablecoins supply circulating digital dollars outside legal tender; CBDC is the sovereign reclaiming of a “default public option.” For on-chain VRC-10-class public-domain money, triangular competition means the advantageous scenes are not replacing CBDC, but corridors beyond the reach of legal tender and CBDC or that regulation prefers not to reach—test with corridor penetration data; do not presuppose from a whitepaper roadmap. Hayek’s Chapter 9 concretizes competitive units as bank-issued competition among distinguishable named currencies; in the protocol era, competition moves up to distinguishable rule suites—whether issuance discipline can be independently verified by third parties, not only comparison of bank names.

Competition between protocol stablecoins and CBDC is more likely at the edge of transmission than on the central bank's internal dealing desk. To test this inference (possibility $\neq$ already happened), at least three observable contrasts help: in high-friction corridors (World Bank 2023 remittance average cost about 6.2%, often above 8% in Sub-Saharan Africa), whether on-chain stable-unit receive intensity is systematically higher than in low-friction economies—Chainalysis' s *2024 Geography Report* shows Argentina, Turkey, and other high-inflation countries with on-chain stablecoin inflows well above the global mean, yet penetration still far below everyday retail fiat¹⁹; in CBDC pilot countries (Nigeria's eNaira, Eastern Caribbean DCash, etc.), active wallets as a share of M2—mostly far below design targets, showing that payment network effects and compliance interfaces remain bottlenecks; in cross-border B2B settlement, latency and total-cost contrasts between permissioned private-domain stablecoins (VRC-11-class) and correspondent banking—no single authoritative panel yet; test corridor by corridor. For the protocol-money path, dialogue with the CBDC literature matters because CBDC may, on whitepaper terms, rewrite the institutional parameters of “who holds risk-free money and how bank liability costs move with policy”; protocol stablecoins supply another readable set of liability and collateral rules on-chain—whether the two complement or substitute at the margin awaits mainnet scale and regulatory precedents, and cannot be presupposed from a whitepaper roadmap.

Section 6. Transmission Blockages: Liquidity Traps and Credit Crunches

Monetary-policy transmission is not frictionless. Under certain macro-financial conditions, the chain breaks at particular nodes, and policy's real effect is heavily impaired or wholly nullified.

The liquidity trap is Keynes' s concept, historically verified in Japan' s “lost decade,” and after 2008 again a policy reality in several economies. When nominal rates fall near zero, further cuts disappear in theory (negative rates face many operational constraints), and monetary policy's price tools approach failure—Woodford and Eggertsson—Woodford formalize this as the effective lower bound (ELB) constraint: under nominal rigidities, moderately positive inflation leaves room for relative-price adjustment, and is one core of the welfare case for a 2% inflation target²⁰. More fundamentally: even with abundant liquidity, if firms are pessimistic about future demand and households anxious about future income, easy credit conditions cannot activate effective borrowing demand. “Banks are not short of funds; no one is coming to borrow” was a true description of Europe and America in 2009–2012 and of Japan years earlier.

A credit crunch is another form of transmission blockage, from the supply side rather than demand. When the banking system suffers large losses and capital is severely impaired, banks actively shrink lending to cut risk-weighted assets, even when the macro rate environment is already easy. The “zombification” of Japanese banking in the 1990s and European bank deleveraging after 2008 are classic cases: the central bank injects liquidity, but liquidity pools inside the banking system and fails to flow to firms and households that need funds. Here monetary policy's “pushing on a string” dilemma appears—the central bank can supply liquidity but cannot force banks to lend or firms to borrow.

Collateral constraints are another important source of blockage. Bank loans usually require collateral, and collateral values co-move with the cycle—in downturns asset prices fall broadly, collateral shrinks, banks tighten standards for prudence, and borrowers who need funds cannot get them, forming a procyclical credit squeeze that amplifies rather than cushions the downturn. This is among the hardest structural defects in monetary transmission, and a key reason fiscal policy is indispensable in crises.

On-chain DeFi protocols offer an interesting contrast in collateral management. Overcollateralized stablecoin protocols such as MakerDAO require borrowers to lock collateral worth 150%–200% of the loan; once the collateral ratio breaches a set threshold, the protocol automatically triggers liquidation with no human decision.

Under normal conditions this effectively prevents bad-debt accumulation; under extreme stress (e.g. “Black Thursday” in March 2020, when ETH fell more than 50% within hours), automatic liquidation itself creates heavy sell pressure, deepens the price fall, triggers more liquidations, and forms an on-chain version of collateral procyclicality. Procyclicality is thus an intrinsic property of credit systems, with no essential difference between on-chain protocols and traditional banks at the base; the difference lies in the speed of collapse and the path of accountability.

Section 7. Forward Guidance: The Art of Managing Expectations

After the 2008 crisis, when policy rates neared the zero lower bound and traditional tools were nearly exhausted, major central banks developed “forward guidance” as a complementary tool. The core idea: even if further cuts are impossible today, a clear central-bank commitment to **keep rates low for a prolonged future period** can compress long rates and the whole yield curve, achieving easing equivalent to further cuts. Friedman was consistently skeptical of such discretion: he favored a legislative rule constraining the money stock to grow at a fixed rate (about 3%–5% a year), arguing this better avoids policy error and expectation-management failure than reliance on central-bank verbal commitment²¹—though history also showed that purely mechanical rules struggle to cope with changes in monetary definitions driven by financial innovation.

Forward guidance comes in calendar-based and state-contingent types. Calendar guidance (e.g. “keep rates low at least through mid-2015”) is simple and easy to communicate, but inflexible; if conditions change, it may trap the bank in a credibility crisis of “broken promises.” Contingent guidance (e.g. “keep rates low until unemployment falls to 6.5%”) ties the commitment to economic goals and is more adaptive, but communication costs are higher and markets may misread. Fed practice in 2012–2014 mixed both approaches with some success, but also lived through communication failures such as the 2013 “taper tantrum.”

Forward guidance reflects a deeper shift in modern monetary policy: policy is increasingly the art of **managing expectations**, beyond pure operating technique. Every word from the governor is parsed by markets; wording shifts after press conferences can reprice global financial assets in seconds. This “language as policy” tendency places extreme demands on communication skill and accumulated credibility, and introduces new fragility: once credibility is damaged, it is not only a particular tool that fails, but the whole expectations-based framework that risks collapse.

Forward guidance and on-chain protocol governance votes form a meaningful functional contrast. The former transmits future-action intent to markets through verbal commitment, its force depending on institutional reputation and external pressure; the latter decides parameter changes through formal voting, with execution guaranteed by code and independent of anyone’s intent. Each has strengths: forward guidance is flexible and can adjust when expected conditions change; on-chain governance decisions are determinate and execute automatically once passed. But on-chain governance faces its own problems—low participation, whale capture, proposal fatigue—so that the ideal of “democratic governance” is heavily discounted in practice. Comparative study of these two expectation-management mechanisms is an important frontier of monetary institutionalism in the coming years.

From a protocol perspective, traditional monetary policy depends heavily on the issuer’s **credible commitment**, which cannot be fully locked in by technical means and must be continually accumulated and maintained over time. That differs sharply from the logic of on-chain protocols that harden rules into contract code—each has its domain of applicability and its distinctive vulnerabilities.

Section 8. Distributional Effects of Monetary Policy and Political Economy

In standard macro textbooks, monetary policy is described as an aggregate tool—adjusting aggregate demand and controlling the overall price level—appearing to act equally on everyone. In reality its effects across groups are markedly heterogeneous; the post-2008 ultra-easy era brought that heterogeneity to the fore and raised questions about the central bank’s political legitimacy. Distributional mechanisms and data (Cantillon paths, asset-wage gaps, concentration of equity holdings) are analyzed systematically in Chapter 3, Section 2¹⁰; this section focuses on structural sources of transmission heterogeneity, and whether on-chain protocols can supply observable alternative constraints.

The asset-price channel is the most direct source of distributional effects: QE compresses long rates and lifts equity and real-estate valuations; high-wealth groups gain especially from asset appreciation, while middle- and lower-income groups that rely on deposits face eroded real returns. Correlation $\neq$ causation—easy periods also coincided with earnings cycles, buybacks, and tax changes—but the testable fact is transmission timing: asset prices respond to liquidity injections earlier than wages. During the Fed’s large-scale easing in 2020–2021, U.S. wealth-Gini-related indicators sat in historically high ranges; the Fed’s *Distribution of Household Wealth* shows that in 2021Q4 the top 10% of households held about 67% of total wealth and about 89% of corporate equity and mutual-fund shares—the distributional fact is verifiable; whether policy “intended” to worsen inequality is a normative judgment and should not be treated as an a priori conclusion²².

The credit channel’s distributional effects likewise deserve attention. Easy policy lowers borrowing costs and in theory benefits all borrowers, but in practice credit access is highly uneven across firm sizes and credit grades. Large listed firms can issue bonds and tap capital markets at very low rates; SMEs depend mainly on bank loans, and banks after crises tend to tighten standards, so the dividend of easy policy is incompletely transmitted. Beck et al.’s (2018) survey of SME finance globally shows that post-crisis bank-standard tightening can lag-hit micro and small firms for years—“dual transmission” has cross-country panel support, not mere narrative²³. This micro differentiation keeps policy intent and actual outcomes persistently apart, and helps explain why “monetary-policy neutrality” is hard to sustain in political discourse.

On-chain protocol issuance rules are equal for all addresses at the code layer—the same collateral ratio, the same liquidation order, the same rate formula—making discriminatory transmission easier to identify in on-chain data than traditional bank credit; on-chain rates are set by contracts and pool supply–demand, without loan-officer discretion. One must admit this is not “barrier-free, non-discriminatory inclusive finance.” Overcollateralized lending requires participants to hold volatile assets first, converting the credit threshold into a wealth threshold; MakerDAO’s liquidations and zero-price auctions on “Black Thursday” 2020, and subsequent governance revisions to liquidation mechanics, show that automatic rules also produce distributional shocks in extreme markets, only along an auditable path.

Claims that on-chain finance is “transparent and consistent for everyone” face two counterexamples. Permissionless CDP protocols by default exclude participants without collateral—different mechanism from bank loan denial, similar result; PCIM converts access from licenses to Bitgold holdings, not eliminating the threshold, only changing its form. Validators/builders can also reorder transactions via MEV (maximal extractable value), so that large liquidations, arbitrage, and front-running precede ordinary users; Flashbots and similar mitigations reduce some visibility but do not eliminate structural advantages at the protocol and infrastructure layers—whales, professional searchers, and early governance large holders enjoy informational and timing advantages in liquidation auctions, governance votes, and liquidity provision. The protocol’s value is not in claiming to “abolish discrimination,” but in making discrimination and incentives observable, measurable, and writable into

improvement proposals—collateral parameters, liquidation penalties, MEV auction revenue attribution, governance quorum and timelocks can all be debated on-chain; traditional credit discrimination is embedded in loan-officer judgment and internal models, hard for outsiders to reproduce. Here one should narrow the claim to verifiability of the constraint carrier, not utopian equality. Without off-chain identity and prudential regulatory interfaces, DeFi still struggles to serve traditional “unsecured retail credit”; full elimination of MEV may require long coevolution of protocol layers and L2 sequencing markets, with no closed theoretical guarantee yet.

When on-chain protocols claim “rules consistent for all, no credit discrimination,” they must simultaneously admit that permissionless CDPs convert credit thresholds into wealth thresholds, and that MEV tilts liquidation and redemption timing toward professional searchers—Aramonte et al. (2021) BIS ex-post analysis lists the “decentralization illusion” alongside oracles, governance, and liquidity concentration as systemic risks; **verifiable** $\neq$ **unbiased**²⁴. Protocol-side responses that can be debated, and questions still open, fall under four points. Permissionless CDPs convert credit thresholds into wealth thresholds—participants must first hold volatile collateral. PCIM’s response is layered, not a claim of “barrier-free for all”: the VRC-10 public-domain layer constrains issuance discipline with Bitgold dynamic-tier overcollateralization (circulation-triggered referenda, upper tier about 161.8%, $C_0 > 100\%$), naturally favoring participants who already hold reserves; the VRC-11 private-domain layer uses permissioned whitelists and off-chain redemption so that supply-chain nodes without Bitgold can still obtain a stable settlement unit within the domain. The threshold shifts from “central-bank license” to “collateral holdings or domain access”; auditability rises accordingly, while whether macro exclusion falls still awaits corridor data. When MEV tilts liquidation, minting arbitrage, and governance votes in timing toward professional searchers, protocol-side mitigations that can be debated include recycling MEV auction revenue to the treasury or insurance fund, L2 fair sequencing markets, and shortening oracle circuit-breaker windows (Lehar & Parlour 2025; Capponi et al. 2024)—discrimination observable is not discrimination eliminable^{25,26}. Barbon and Rinaldo (2024) show that DEX peg repair is slower than CEX when gas fees are high and depth thin; PCIM redemption-arbitrage chains must therefore bring cross-venue liquidity into observable metrics rather than assume a single continuous OTC market²⁷. Chitra et al.’s (2024) DAISIM simulation of DAI shows that even overcollateralized CDPs still depend on a “belief parameter” for the peg—when confidence in redemption executability falls, the wealth threshold and peg fragility amplify together; PCIM must, on whitepaper terms, write collateral ratio C_0 , reserves R , and redemption-channel depth into observable metrics, not merely claim transparent rules. If governance unilaterally eases the output ratio (cuts C_0) or expands the balance sheet outside crisis without a referendum, it must satisfy split-track quorum, timelock, and other engineering constraints, or “verifiable rules” die in capture; circulation up-tiers require a trigger referendum, and if it fails the prior tier is maintained; crisis tightening separately requires a referendum to raise C_0 and lower σ (Chapter 14, Section 2.2). Still unclosed: L1 proposer-builder separation has no theoretical guarantee of zero MEV; “redemption run + MEV front-running redemptions” can stack in extreme markets (VRC-10 rules in the glossary), awaiting practical tests rather than whitepaper presupposition. Auer et al.’s (2023) BIS post-mortem of the DeFi stack shows that concentrated selling of Terra/UST in Curve pools can trigger a chain-wide run within hours—thin pools + MEV timing advantage still tilt “consistent rules” toward professional searchers in distribution²⁸. Open questions remain: Aspris (2024) empirics on Maker vault-level leverage show that wealth thresholds and over-leverage hurt low-skill participants especially—PCIM’s layered thresholds (VRC-10/11) are observable; whether they reduce macro exclusion still awaits corridor data; MEV observable is not MEV eliminable.

注释与引用

1. Federal Reserve FOMC statements and dot plot: hiking from 2022-03-16, target range 5.25%–5.50% as of 2023-07-26 (FRED FEDFUNDS / DFEDTARU); 30-year mortgage peaks in Freddie Mac PMMS 2022–2023 series. People's Bank of China: February, September, and December 2024 RRR cuts of 0.5 percentage points each, releasing long-term funds on the order of RMB 1 trillion cumulatively (PBOC press releases and monetary-policy reports). ↩ ↩²
2. Holston, Laubach & Williams (2017), "Measuring the Natural Rate of Interest," *International Journal of Central Banking* 13(5), pp. 55–76 (U.S. r^* from ~3%–4% in the 1980s to near zero in the 2010s); BIS WP 1067 (2023), "Estimating the natural rate of interest in an open economy," §§2–4 (cross-country r^* decline and model sensitivity). <https://www.bis.org/publ/work1067.htm> ↩
3. Friedman (1968), "The Role of Monetary Policy," p. 12: "It cannot use its control over nominal quantities to peg a real quantity—the real rate of interest, the rate of unemployment, the level of real national income ..." PDF: https://www.cooperative-individualism.org/friedman-milton_the-role-of-monetary-policy-1968-mar.pdf ↩
4. Compounding Finance / Gauntlet and others' 2020–2021 reviews of DeFi lending rates: COMP and similar liquidity-mining subsidies depressed observed rates; after subsidies faded, Aave/Compound rates repriced; see Gauntlet "DeFi Risk Dashboard" series and SEC 2022 enforcement cases on certain yield products (subsidy $\neq$ equilibrium rate). ↩
5. Bank of England (2014), "Money creation in the modern economy," *Quarterly Bulletin* 2014 Q1, pp. 14–27: "Money multiplier ... misleading ... loans create deposits." <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy> ↩ ↩²
6. Fisher (1911), *The Purchasing Power of Money*, ch. 2: brings money (M) and check deposits (M') into the equation of exchange $MV + M'V' = PT$, and systematically argues that the quantity theory is "fundamentally sound" but must incorporate deposit media. English edition: <https://fraser.stlouisfed.org/title/purchasing-power-money-5379> ↩
7. Brunnermeier & Niepelt (2019), "On the Equivalence of Private and Public Money," *Journal of Monetary Economics* 106, pp. 27–41; Bindseil (2020), "Tiered CBDC and the Financial System," ECB WP 2351, §§3–4 (tiered remuneration): <https://www.ecb.europa.eu/pub/pdf/scpwp/ecb.wp2351~c8c18bbd60.en.pdf>; Assenmacher & Smets (2024), SUERF Policy Note 346, §§1–5: <https://www.suerf.org/publications/suerf-policy-notes-and-briefs/a-digital-euro-monetary-policy-considerations/> ↩ ↩²
8. Niepelt (2024), "Money and Banking with Reserves and CBDC," *Journal of Finance* 79(4), pp. 2505–2552 (optimal differentiation of CBDC and reserve rates, payment-share calibration); Brunnermeier & Niepelt (2019), "On the Equivalence of Private and Public Money," *Journal of Monetary Economics* 106, pp. 27–41 (equivalence premises). <https://www.niepelt.ch/files/jf2024.pre.pdf> ↩
9. Chiu, Jonathan, Seyed Mohammad R. Davoodalhosseini, Janet Hua Jiang, and Yu Zhu. "Bank Market Power and Central Bank Digital Currency: Theory and Quantitative Assessment." *Journal of Political Economy* 131(5), May 2023, pp. 1213–1248 (orig. Bank of Canada Staff Working Paper 19-20, 2019; CBDC as deposit outside option, credit and output effects); Andolfatto, David. "Assessing the Impact of Central Bank Digital Currency on Private Banks." *Federal Reserve Bank of St. Louis Review* 103(2), 2021, pp. 153–175; Brunnermeier, Markus K., and Yann Koby. "The Reversal Interest Rate." *American Economic Review* 109(8), August 2019, pp. 2615–2647; Agur, Itai, Anil Ari, and Giovanni Dell'Ariccia (2019), IMF WP 19/252, §§III–IV. <https://doi.org/10.1086/722075> ; <https://www.stlouisfed.org/publications/review/2021/02/05/assessing-the-impact-of-central-bank-digital-currency-on-private-banks> ; <https://doi.org/10.1257/aer.20181007> ↩ ↩² ↩³
10. QE data and distributional analysis in Chapter 3, Section 2¹⁴, Chapter 1, Section 6²¹; Bernanke (2015), *The Courage to Act*, chs. 7–9 (three QE rounds' scale, long rates, and employment lags); Federal Reserve H.4.1 balance-sheet series. <https://www.federalreserve.gov/monetarypolicy/bst.htm> ↩ ↩² ↩³
11. FDIC (2023-03-12), "FDIC Creates a Deposit Insurance National Bank of Santa Clara ... Silicon Valley Bank, Santa Clara, California, Closed Today"; SVB 2022 Form 10-K: AFS securities about \$91 billion, unrealized losses about \$15.1 billion as of December 31, 2022 (SEC EDGAR). <https://www.fdic.gov/news/press-releases/2023/pr23016.html> ↩
12. Bernanke & Gertler (1995), "Inside the Black Box: The Credit Channel of Monetary Policy Transmission," *Journal of Economic Perspectives* 9(4), pp. 27–48; Federal Reserve SLOOS 2007Q3–2009Q1 loan-standard tightening series (FRED); Gilchrist & Zakrajšek (2012), "Credit Spreads and Business Cycle Fluctuations," *American Economic Review* 102(4), pp. 1692–1720. <https://doi.org/10.1257/aer.102.4.1692> ↩ ↩²

13. Friedman (1968), "The Role of Monetary Policy," p. 11: the temporary trade-off "comes not from inflation per se, but from unanticipated inflation, which generally means, from a rising rate of inflation." PDF: https://www.cooperative-individualism.org/friedman-milton_the-role-of-monetary-policy-1968-mar.pdf ↩
14. Bernanke et al. (1999), *Inflation Targeting: Lessons from the International Experience*, chs. 1–2 (institutionalizing inflation targets and anchoring expectations); Clarida, Gali & Gertler (1999), "The Science of Monetary Policy," *Journal of Economic Literature* 37(4), pp. 1661–1707 (survey of New Keynesian reaction functions). <https://doi.org/10.1257/jel.37.4.1661> ↩ ↗²
15. Taylor (1993), "Discretion versus Policy Rules in Practice," *Carnegie-Rochester Conference Series on Public Policy* 39, pp. 195–214; Leeper (1991), "Equilibria under 'active' and 'passive' monetary and fiscal policies," *Journal of Monetary Economics* 27(1), pp. 129–147; Sargent (1982), "The Ends of Four Big Inflation," *Inflation: Causes and Effects*, pp. 41–98; Sargent & Wallace (1981), "Some Unpleasant Monetarist Arithmetic." [https://doi.org/10.1016/0167-2231\(93\)90009-L](https://doi.org/10.1016/0167-2231(93)90009-L) ; [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ↩ ↗² ↗³
16. Sargent (1999), *The Conquest of American Inflation*, chs. 2–3: Volcker tightening and rebuilding the inflation anchor under rational expectations. Princeton University Press, 1999. ↩
17. Bindseil (2020), "Tiered CBDC and the Financial System," ECB WP 2351, §§3–5 (tiered rates, holding thresholds); Agur, Ari & Dell' Ariccia (2019), IMF WP 19/252, §§III–IV (CBDC rate and holding-cap trade-offs); Meller & Soons (2024), ECB OP 326 "Know your (holding) limits," abstract and §5 (€3,000 per-person cap, 2000+ bank simulation); Niepelt (2024), *Journal of Finance* 79(4), pp. 2505–2552 (optimal differentiation of CBDC and reserve rates). <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf> ; <https://www.imf.org/en/Publications/WP/Issues/2019/09/26/Designing-Central-Bank-Digital-Currencies-48655> ; <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op326~d5c223d9b4.en.pdf> ↩ ↗² ↗³
18. BIS Committee on Payments and Market Infrastructures (2022), *Stablecoins: Implications for monetary policy, financial stability and the international monetary system*, §§II–III (stablecoin scale and CBDC policy responses); Brunnermeier, James & Landau (2019), BIS WP 941, §5.2 (platform-money triangle). <https://www.bis.org/publ/othp31.htm> ↩
19. World Bank (2023), *Remittance Prices Worldwide* Q3, global average about 6.2%, SSA corridors often above 8%; Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*, on-chain stablecoin inflow intensity in Argentina, Turkey, etc. (penetration still far below retail fiat; not to be read as monopoly already broken). <https://remittanceprices.worldbank.org/> ↩
20. Woodford (2003), *Interest and Prices*, chs. 6–7 (ELB and optimal inflation); Eggertsson & Woodford (2003), "The Zero Bound on Interest Rates and Optimal Monetary Policy," *Brookings Papers on Economic Activity* 2003(1), pp. 139–211. <https://doi.org/10.1353/eca.2003.0010> ↩
21. Friedman (1962), *Capitalism and Freedom*, p. 54: advocates legislation requiring the money stock to rise "month by month ... at an annual rate of X%, where X is some number between 3 and 5." University of Chicago Press, 1962. ↩ ↗²
22. Federal Reserve Distributional Financial Accounts (former Flow of Funds household distribution tables), 2021Q4: top 10% held about 67% of total wealth and about 89% of corporate equity & mutual fund shares (Z.1 DFA Table B.101hn). <https://www.federalreserve.gov/releases/z1/data/dfa/distributional-financial-accounts.xlsx> ↩
23. Beck, Demirgüç-Kunt & Peria (2018), "Bank Financing for SMEs around the World," *Journal of Financial Perspectives* 6(3): post-crisis bank credit standards' lagged hit on micro and small firms; consistent with SLOOS micro measures. ↩
24. Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf (2021), "DeFi risks and the decentralisation illusion," *BIS Quarterly Review*, December 2021, pp. 21–36: oracles, governance, and liquidity concentration; verifiable ≠ de-risked; Aspris (2024), SSRN WP 4913633: Maker vault-level leverage and harm to low-skill participants. https://www.bis.org/publ/qtrpdf/r_qt2112e.htm ; <https://ssrn.com/abstract=4913633> ↩
25. Capponi, Jia & Wang (2024), "The Evolution of Market Structure in DeFi," *Management Science* forthcoming preprint: DEX liquidity concentration, MEV, and structural searcher advantage; Cong, Li & Wang (2024), *Journal of Financial Economics* 151: tokenomics dynamic adoption and subsidy sustainability; Chitra et al. (2024), *Frontiers in Blockchain* 7, 1392812: DAISIM simulation, DAI peg belief parameters, and ETH collateral risk. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4273980 ↩
26. Lehar, Alfred, and Christine A. Parlour. "Decentralized Exchange: The Uniswap Automated Market Maker." *Journal of Finance* 80(1), February 2025, pp. 321–374: AMM pool equilibrium and large-holder rebalancing; Qin et al. (2021), "An empirical study of DeFi liquidations," *IMC 2021: longitudinal MakerDAO liquidation data*. <https://doi.org/10.1111/jofi.13405> ; <https://arxiv.org/abs/2106.06389> ↩

27. Barbon, Andrea, and Angelo Rinaldo (2024), "On the Quality of Cryptocurrency Markets: Centralized versus Decentralized Exchanges," *Management Science* forthcoming; arXiv:2112.07386: CEX/DEX liquidity quality, gas fees, and arbitrage deviations; complements Ferraro, Kan & Sunderam (2022) thin-market peg analysis. <https://arxiv.org/abs/2112.07386> ↩
28. Auer, Raphael, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese, and Friedhelm Victor (2023), "The Technology of Decentralized Finance (DeFi)," BIS Working Paper 1066, §4 (Terra/UST Curve-pool run and thin DEX pools); Capponi, Jia & Wang (2024), "The Evolution of Market Structure in DeFi": MEV and structural searcher advantage. <https://www.bis.org/publ/work1066.htm> ↩

§ 10 The Boundary Between Fiscal and Monetary Policy

However refined monetary-policy tools become, they cannot escape the boundary between fiscal and monetary policy—a boundary repeatedly probed in crises.

In textbook macroeconomics, fiscal and monetary policy are two independent toolkits: the finance ministry handles taxes and spending; the central bank handles money supply and interest rates. Behind that division lie solid institutional logic and hard historical lessons—an attempt to separate expansionary political power from money-creating capacity with inflationary effects. In practice the boundary has never been as sharp as theory draws it, and under extreme pressure it melts with unsettling speed. Debt monetization, fiscal dominance, Modern Monetary Theory—these terms mark different moments when the boundary was questioned or breached. This chapter traces the institutional logic and historical evolution of that boundary, and tries to understand the structural challenges it faces from a protocol perspective.

Section 1. The Logic of Separation: Why Distinguish Fiscal from Monetary Policy

Japan after the 1990s long practiced “fiscal–monetary coordination”: the government issued large volumes of JGBs, and the Bank of Japan continuously bought them in the secondary market—by end-2023 the BOJ held about ¥581 trillion of JGBs, roughly 52% of the outstanding stock (Bank of Japan *Monthly Report* series), functionally close to monetizing the fiscal deficit, even though legal texts still distinguish primary- from secondary-market operations¹. When Bernanke visited Japan in 2013 he used “helicopter money” as a metaphor for more aggressive fiscal–monetary joint action—a phrase later widely cited, and one that also stirred fears of the central bank becoming a fiscal financing machine. A distinction is required: secondary-market bond purchases may be institutionally “detachable” from fiscal financing, yet under persistently high holdings they are often hard to detach “in reality”—a contemporary sample of the boundary as “limited constraint” rather than “complete isolation.”

Separating the power to issue money from government fiscal power is, at root, an institutional design against an ancient temptation: government can always print money to pay its bills. From Roman emperors debasing coin, through early-modern European monarchs authorizing central banks to over-issue paper for war finance, to twentieth-century hyperinflation cases—monetary history shows that combining political power with money-creating capacity has never delivered long-run monetary stability. The temptation of issuance is especially hard to resist because its cost (inflation) typically lags its benefit (immediate purchasing power), and in democratic politics the pressure of the next election usually outweighs abstract worry about future inflation.

The core of separation design is an institutional solution to the time-inconsistency problem: delegate monetary policy to an independent institution, give it a clear price-stability mandate, and wall off political intervention by law and institutional arrangement. An independent central bank is not bound by the electoral cycle and can take measures that are unpopular in the short run but beneficial to stability in the long run—for example raising rates and slowing the economy briefly to break an inflation uptrend. The effectiveness of this arrangement was validated to a considerable degree in the “Great Moderation” of the 1990s–2000s: major advanced economies achieved both low inflation and relatively mild fluctuations.

Yet the other side of fiscal–monetary separation is that the separation is forever incomplete at the institutional level. Government debt levels, tax policy, and fiscal deficits continuously shape the environment of monetary policy through long rates, risk premia, and economic structure; monetary-policy rate decisions, by affecting the cost of servicing government debt, constrain fiscal space in turn. Two policy domains that should be

independent remain deeply coupled in macroeconomic reality. Recognizing that coupling cannot be eliminated does not deny the value of separation; it only requires a realistic view of its limits: the institutional aim is limited constraint on political intervention, not complete isolation. That realist lens is equally necessary caution when assessing whether on-chain protocols can truly cut the fiscal–monetary boundary at the root.

Independence itself is fragile. Whatever the legal wording, appointment of the governor, day-to-day coordination with the finance ministry, and pressure from government rescue requests in crises are real channels through which politics penetrates monetary policy. Deeper still: under extreme fiscal stress—war, major crisis, debt-sustainability crisis—insisting on central-bank independence may be treated as an institutional luxury. Tension between institutional logic and political reality runs through the entire history of independent central banks from their founding to today.

Section 2. Seigniorage: The Fiscal Dividend of Money Issuance

Seigniorage is the most direct fiscal–monetary boundary question. Originally it meant the mint’s profit margin from coinage: face value exceeding metal content plus minting cost, the difference accruing to the issuer. In the modern sense seigniorage usually means the central bank’s comprehensive return from issuing money: the bank issues money at zero (or near-zero) cost, buys interest-bearing assets (usually government bonds) with it, and remits most interest income net of operating costs to the treasury. In 2023 the Federal Reserve transferred about \$7.6 billion to the Treasury (a low level after post-pandemic rate rises compressed securities-portfolio returns; the 2015 peak exceeded \$97 billion), and the Eurosystem remitted about €7.6 billion (2023)—the most routine interest link between central bank and fisc².

Seigniorage in this normal state is relatively benign: money-supply growth matches economic growth and the price level; issuance revenue flows into the treasury in a predictable way without destroying monetary stability. The problem is “unconventional seigniorage” when government needs large financing—directly ordering the central bank to buy government bonds and funding the fiscal deficit with money issuance. That is financing government by diluting all money holders’ purchasing power: the essence of the inflation tax. Friedman defined inflation precisely as a monetary phenomenon: “Inflation is always and everywhere a monetary phenomenon,” its proximate cause money growing faster than output available for expenditure³—seigniorage and debt monetization are the institutionalized outlets of that mechanism under fiscal pressure.

The beneficiary structure of seigniorage differs fundamentally between modern fiat systems and on-chain protocol systems—a difference worth close attention. In fiat systems, seigniorage flows to public finance—the purchasing power of newly issued money is effectively transferred from all existing holders to government, which uses it to pay public wages, infrastructure, and services. The transfer is opaque, not explicitly recorded in any fiscal account, and therefore lacks transparent political accountability. In on-chain protocols, newly issued tokens are usually allocated through explicit incentive mechanisms: mining rewards to miners (Bitcoin), staking rewards to validators (Ethereum), liquidity rewards to liquidity providers (DeFi protocols). Those allocation rules are public at the protocol layer; holders can know who benefits from issuance before they participate. Seigniorage allocation shifts from a hidden fiscal tool to an open economic incentive design—one of the most salient structural differences of on-chain money protocols in institutional transparency.

The classic historical cases are war finance: Britain in both world wars required the Bank of England to finance wartime deficits directly or indirectly; the United States in World War II required the Fed to keep rates low under a “Treasury support” arrangement, in effect suppressing monetary-policy independence. After the war the core question for each country was how to rebuild monetary-policy independence in peacetime and distinguish normal seigniorage from wartime unconstrained monetization. That reconstruction proceeded at

different speeds in different countries, and the difficulty of reconstruction itself shows that once fiscal penetration of money begins, reversal exacts a heavy political price.

Section 3. Debt Monetization: Historical Cases and Institutional Controversies

Debt monetization means the central bank buys government bonds and in substance provides direct financing for the fiscal deficit, expanding base money. At the institutional-design level, many advanced economies' laws explicitly forbid the central bank from buying newly issued government bonds in the primary market (direct monetization), while allowing secondary-market purchases of already issued bonds (indirect operations such as QE)—a distinction often nearly equivalent in economic effect, yet vastly different in political meaning.

Weimar hyperinflation (1921–1923) is the historical template of monetization out of control. Postwar Germany faced astronomical reparations; revenue fell short of spending, and parliament could not reach political consensus on tax increases or spending cuts. The eventual “solution” was to let the Reichsbank print without limit to pay government bills. In 1923 the mark's exchange rate fell to about one 4.2-trillionth of its prewar level; wheelbarrows of notes for shopping and notes burned as fuel became permanent warning images in monetary textbooks. Hyperinflation destroyed middle-class savings and laid groundwork for Weimar's political collapse—many historians see it as an important background factor in the rise of the Nazi movement. Fisher early noted that increases in the quantity of money are “among the most common causes” of disturbing equilibrium and setting off price oscillations⁴—Weimar concretized that quantity-theory proposition in the most catastrophic way.

Weimar hyperinflation was not an overnight loss of control, but a gradual slide into the abyss through mutually reinforcing political bargaining and path dependence. Once printing begins to fund the fisc, inflation expectations are priced into wage bargaining and pricing decisions early, pushing prices higher and forcing government to print still more to fund the same real spending—a self-accelerating positive-feedback loop. Each step looks unavoidable until the monetary system's credibility collapses entirely. That path dependence makes monetization extremely hard to stop once started, whatever the ex-ante political intention. Designers of on-chain issuance mechanisms need to internalize this path-dependence risk in protocol design, rather than leave a promise of “we will not make wrong decisions” to future governance participants.

By contrast, postwar West Germany established a Bundesbank regime that unusually emphasized central-bank independence and price stability, institutionalizing historical fear of inflation as a core feature of German political culture. The ECB's design was deeply marked by Bundesbank DNA, stressing price stability even more than the Fed or the Bank of England. Fisher's “compensated dollar” proposal in *Stabilizing the Dollar*—periodically adjusting gold content by a price index so that the dollar's purchasing power rather than metal weight stays constant⁵—did not become the postwar institutional choice, yet its claim that price stability should take priority over exchange-rate rigidity runs in the same line as the Bundesbank. That difference deeply shaped the ECB's slow response in the euro debt crisis and Germany's hard line toward peripheral fiscal distress—historical memory leaves institutional marks in monetary regimes.

More contested in recent years are major central banks' large-scale asset purchases after 2008 and after 2020 (QE mechanisms and distributional consequences in Chapter 3, Section 2)⁶: critics argue that once the central bank holds a material share of outstanding government debt, functional monetization is hard to deny—the Fed holds about 24% of U.S. Treasuries (2024 H.4.1 basis), the ECB's holdings of euro-area member sovereign debt peaked in a post-crisis range of about 20%–33% (ECB *Statistical Bulletin*), and the BOJ's share is higher still¹⁶. Supporters stress that under deflation risk and the zero lower bound, this was a necessary tool for financial stability and policy goals. The debate shows that the fiscal-monetary boundary takes starkly different faces at different historical moments.

Section 4. Modern Monetary Theory: A Direct Challenge to the Boundary

If traditional economics treats the fiscal–monetary boundary as an important institutional achievement to be guarded, Modern Monetary Theory (MMT) treats that boundary as a harmful cognitive error. MMT’s core proposition can be summarized: for a country with monetary sovereignty—issuing its own currency, denominating debt in that currency, floating the exchange rate—the fundamental constraint on government spending is the real economy’s resource capacity (i.e. inflation), not the funding source itself.

MMT’s reasoning runs as follows: a monetarily sovereign government never faces true “fiscal bankruptcy” risk, because it can create money through the central bank to pay any domestic-currency obligation; taxation’s main functions, in MMT’s account, are to create demand for the domestic currency (tax obligations drive public acceptance of fiat) and to restrain inflation (withdrawing money from the private sector); government spending itself does not presuppose tax revenue; issuing Treasuries is characterized as maintaining safe-asset supply and managing banking-system reserves, not financing in the traditional sense.

MMT’s policy recommendations received considerable political attention in the early 2020s: if government can spend without fiscal constraint, why not use that for a job guarantee, green infrastructure, and greatly expanded social welfare? Its fashion in progressive U.S. political circles coincided with large-scale fiscal stimulus as a real experiment in the pandemic. The global inflation comeback of 2022 posed, to a degree, an empirical challenge to the experimental character of 2020–2021 large fiscal–monetary expansion—even if theoretical supporters insist the cause was supply-chain shocks rather than monetary–fiscal excess, the political shock was real and drove a broad reassessment of MMT recommendations.

Yet MMT has been widely criticized by mainstream macroeconomists. Critics note that MMT confuses technical feasibility with economic sustainability—government can print in a technical sense, but monetary expansion faster than output growth necessarily produces inflation; the inflation constraint is hard to identify and regulate precisely in practice, and once inflation runs away, the cost of tightening (recession and unemployment) is often nonlinear; monetary sovereignty itself is fragile—once inflation damages currency credibility, capital flight and depreciation rapidly expose resource constraints in extreme form, and small open economies are especially vulnerable. Friedman and Schwartz’s study of the Great Depression in *A Monetary History of the United States* showed that monetary forces can amplify an avoidable contraction into a prolonged depression —“the contraction is in fact a tragic testimonial to the importance of monetary forces”⁷—a historical verdict often used against the optimistic assumption that “fiscal expansion can come without an inflation cost.” MMT describes local truths under certain conditions, but universalizing those local truths into a general policy framework ignores countless historical cases of fiscal–monetary discipline collapse. Possibility ≠ actuality is especially critical here: accounting identities may “possibly” hold on paper; actuality depends on tax-base breadth, central-bank independence, and capital-account openness—economies that satisfy all three at once are far fewer in the sample than MMT policy discourse implies; the 2022 inflation rebound and cases such as Turkey and Argentina are observable counterexamples, not exceptions that rhetoric can dissolve.

Section 5. The Risk of Fiscal Dominance: Latin American Lessons

“Fiscal dominance” is the economics term for fiscal policy overriding monetary policy: when the government’s debt-sustainability needs dominate the course of monetary policy—the central bank forced to keep rates low to compress debt-service costs, or forced to buy Treasuries to avoid default—monetary policy becomes in substance an auxiliary of fiscal policy, and the price-stability objective retreats to secondary status.

Latin America supplies the densest historical cases of fiscal dominance. In the second half of the twentieth century, Argentina, Brazil, Bolivia, Peru, and others repeatedly experienced hyperinflation cycles with strikingly

similar common pathology: governments relied on expansionary fiscal spending to maintain political legitimacy; a thin tax base produced chronic deficits; the central bank under political pressure continuously financed the deficit; credit expansion briefly stimulated boom; then runaway inflation and depreciation wiped out savings; economic crisis bred political instability, which further deepened the fiscal crisis—a vicious circle.

Brazil's story has its own historical layers. Between 1985 and 1994 Brazil underwent multiple monetary reforms and failed stabilization plans, with cumulative inflation reaching astronomical rates. People developed strategies against inflation: wage indexation to price indexes to preserve real purchasing power; goods priced in dollars at the shop counter; beans and other storable goods used as temporary stores of value. The 1994 Plano Real finally achieved stability; the core mechanism was introducing a new monetary unit to replace the old, backed by foreign-exchange reserves to support the conversion rate, cutting the self-fulfilling loop of inertial inflation expectations. Brazil's experience still resonates: reconstructing monetary order involves technique, but still more confidence and politics—often external force (a dollar anchor, an IMF program) is needed to form a sufficiently credible commitment. A limited analogy from this angle suffices: foreign-exchange reserves in the Plano Real were held by the sovereign, used to intervene in the exchange rate and back the conversion promise; Bitgold is a market-priced on-chain volatile asset, and PCIM constrains Bitcurrency issuance with dynamic-tier overcollateralization (upper tier about $C_0 \approx 161.8\%$)—similar in “supplying an exogenous anchoring narrative in institutional transition,” but not interchangeable: Bitgold has no sovereign intervention balance sheet, nor a central bank as lender of last resort.

Argentina is among the most representative cases. In the early twentieth century Argentina was one of the world's richest economies, with per-capita income comparable to Australia and Canada. A century of repeated fiscal mismanagement and currency crises then dragged it gradually into the middle-income trap, replaying historical cycles in the 2001 default and recent persistent inflation. Economists study Argentina, in a sense, as a study of the long decline path a normally functioning economy faces when the fiscal-monetary boundary is completely lost.

Venezuela is the most extreme twenty-first-century case: after oil revenue collapsed, the government printed at massive scale to sustain socialist welfare spending; the IMF estimates the 2018 inflation peak at about 130,060% (year-end year-on-year); the monetary system had in effect already collapsed, and dollars and crypto assets became the de facto money of ordinary people⁸. This is not sealed history—it was still unfolding as this book was written. When formal money loses its store-of-value function, people spontaneously seek substitutes—Chainalysis's 2024 *Geography Report* shows Venezuela's on-chain stablecoin receive intensity well above the global mean, an economic choice forced by high inflation and capital controls, not “monopoly already loosened” as technology-optimist narrative would imply⁹. Observable indicators (on-chain receive intensity, domestic-currency circulation share, degree of dollarization) here beat whitepaper roadmaps: actuality must be tested with penetration and compliance friction; mere technical possibility of holding is not enough to prove that institutional boundaries have been replaced by protocols.

Section 6. The Euro Debt Crisis: A Stress Test of the Institutional Boundary

The euro debt crisis (2010–2015) was among the severest stress tests of fiscal-monetary separation. The euro area's institutional design deliberately maintained strict separation: the ECB runs unified monetary policy; member states retain independent fiscal powers but must observe deficit and debt ceilings under the Stability and Growth Pact. The logic: credibility of a single currency requires each member to keep fiscal discipline; the ECB may not finance any member directly (the “no-bailout clause”).

Yet the crisis' s actual course quickly exposed structural flaws in that design. Greece, Portugal, Ireland, Spain, and Italy successively faced debt-sustainability crises; sovereign yields soared; markets began to price euro-area breakup. The critical problem: these countries had no national central bank and could not print their way out; yet the ECB' s treaty constraints forbade direct purchases of member sovereign debt to compress rates. The framework showed a double bind under crisis: members could not use monetary-policy tools, and the ECB was not allowed to act as the last fiscal backstop.

The unlock came in July 2012, when ECB President Draghi delivered the famous “whatever it takes” speech and then launched Outright Monetary Transactions (OMT)—a commitment to buy troubled sovereign debt in unlimited amounts under specified conditions. The commitment itself was almost never actually used, yet the promise alone calmed market panic, showing the enormous force of central-bank credit as the ultimate anchor of financial stability. Critics noted that OMT in substance broke the institutional promise of the “no-bailout clause,” making the ECB a de facto fiscal backstop; the monetary–fiscal boundary was redrawn under crisis pressure. Draghi' s decision is widely seen as the critical act that saved the euro area, and also as a lesson in how fragile institutional boundaries prove when faced with reality.

Section 7. A Protocol Perspective: How Code Redraws the Boundary

In traditional monetary systems, the fiscal–monetary boundary depends on human-set institutional rules, legal texts, and the maintenance of organizational culture. As prior sections show, that boundary is repeatedly eroded under extreme pressure—sometimes from necessity, sometimes from political opportunism, sometimes from internal contradictions in institutional design. The boundary' s fragility ultimately rests on the fact that the force maintaining it is human will, and human will is continuously shaped by incentive structures and political reality.

Blockchain protocols by design offer a different approach to setting the boundary—to be strictly distinguished from the reality of systems already in production. In an idealized on-chain money protocol, “monetary policy”—supply curves, issuance rates, inflation rules—can be written into contract logic; changes require governance consensus or hard forks and other public procedures; there is no institutional channel by which a legislature' s decree can authorize central-bank bond buying, or a finance minister' s phone call can demand “cooperation” in suppressing rates. Rules are executed by the node network; any single political power' s ability to overwrite rules is technically limited at the protocol layer. Counterexamples are equally real: Ethereum' s 2022 Merge changed the issuance curve; MakerDAO repeatedly adjusted stability fees and liquidation parameters through governance; Terra/UST expanded the balance sheet algorithmically until collapse—code can change, governance can be captured, oracles can fail; “hard-coded discipline” is not yet a verified institutional fact. One should therefore not take “on-chain = boundary unerodable” as an a priori conclusion. A safer formulation: when core issuance parameters are readable by third parties and changes require visible governance procedures, hidden seigniorage and opaque balance-sheet expansion should be politically harder to conceal than in fiat systems—an inference that still needs empirical contrast with mainnet scale, governance participation, and regulatory interfaces, and cannot be read straight from a whitepaper.

That does not mean on-chain protocols have no fiscal–monetary confusion. Many token projects modify economic parameters by governance vote, subsidize operators with new issuance, and affect market circulation through “protocol treasury” spending—operations that in economic nature do not differ essentially from traditional fiscal–monetary confusion. The difference is that these operations are in principle visible, auditable, and must be approved by coded governance procedures, rather than political deals completed in closed rooms—in principle is not in practice: low-participation governance, whale voting, and MEV front-running can all make

“public procedure” hollow. Transparency does not guarantee correct decisions, but it changes the nature and difficulty of accountability; whether it changes them must be tested with observable indicators such as proposal pass rates and the timing correlation of parameter changes with off-chain fiscal events.

Openverse documentation instantiates PCIM as VRC-10 (Bitcurrency, public-domain money) and VRC-11 (Privcurrency, private-domain stablecoin): the public-domain layer is constrained by Bitgold dynamic-tier overcollateralization (circulation-triggered referenda adjusting σ , upper tier about 161.8%) ($C_0 > 100\%$), decoupled from any single actor’s fiscal condition; the private-domain layer uses 61.8% low collateralization plus firm reputation, whitelists, and off-chain redemption—public- and private-domain collateral parameters must not be conflated. The mechanism itself—verifiable collateral and mint/redeem rules replacing institutional promises—belongs with DAI and USDC in a comparable stable-asset spectrum; Openverse here is a deployment sample; open questions include whether oracle TWAP and circuit breakers can close the peg, procyclical expansion when multiple issuers share BTG collateral, and whether redemption channels dry up together with fiat OTC in a sovereign-scale liquidity crisis. Its significance is reopening the answer space for “where monetary discipline comes from”; conclusions still require court judgments, crisis stress tests, and large-scale practice.

Section 8. Academic Rebuttals: Chartalism, New Keynesianism, and MMT

Mainstream macroeconomics has three strongest lines of defense for “protocols cannot replace the mint prerogative”; the following responds to them together, with the 2% inflation target and institutional foundations developed further.

Chartalism: the tax anchor and lender of last resort are irreplaceable. The strongest Knapp–Innes–Wray version holds that money’s value comes first from the sovereign unit of account and the rigid demand created by tax recovery; in crisis the lender of last resort must inject liquidity on state credit—hence protocol money may long remain marginal in retail and public finance, and can scarcely alone bear a March 2020-style market-wide synchronized deleveraging. Response: the tax anchor explains fiat demand and who buffers crises; it does not automatically imply that the mint prerogative must be monopolized; the protocol path supplies auditable parallel discipline, not Bagehot-style unlimited injection (Goodhart 1998; Mehrling 2011; Maker D3M as a limited-corridor contrast). IMF GFSR (2022) Chapter 2 classifies Terra/UST as a systemic-risk sample of algorithmic stablecoins¹⁰; the protocol path must therefore complete Catalini et al.’s (2021) mechanism taxonomy before talking competition. Goodhart (1998) and Brunnermeier–Niepelt (2020) show that the debate’s focus is clearing recovery and rule verifiability, not the ontology of money. Fiat dominance in domestic retail and public spending can coexist for a long time, but “rigid domestic-currency demand” does not automatically entail mint monopoly. In cross-border B2B, open-source ecosystem internal settlement, machine-agent payments, and similar scenes, participants can voluntarily choose verifiably collateralized stable units without waiting for legal-tender status—historically commercial paper and the Eurodollar market expanded outside legal tender. The protocol path offers an optional unit-of-account layer and auditable issuance discipline, not overnight replacement of tax obligations. As for the lender-of-last-resort function, on-chain protocols have no equivalent unlimited-injection actor in a system liquidity crisis—March 2020 MakerDAO and the Fed are not interchangeable: the same day ETH fell about 30%+ and triggered Maker’s liquidation spiral and zero-price auctions, with DAI at a premium; the Fed injected liquidity into the whole banking system via repo and balance-sheet expansion¹¹. The claim therefore does not include “protocols replace the central bank’s crisis function”; it only claims that in particular scenes verifiable overcollateralization and mint/redeem discipline can substitute part of the function of “hidden seigniorage + opaque balance-sheet expansion.” One must still admit: the protocol layer has no institutionalized power to “lend without limit on state credit”; in crisis there are only circuit-breaker pauses, reserve burn-down, governance pauses, and voluntary top-ups by participants—when the whole market deleverages in sync and fiat liquidity also

dries up, on-chain redemption channels and OTC depth may fail together; protocols cannot break the deadlock with political backing the way a Bagehotian lender of last resort can. When reserve quality and volatility are incompletely observable to holders (Ahmed, Aldasoro & Duley 2024), even on-chain disclosure of collateral ratio C_0 and reserve ratios may not prevent coordinated exit under a negative public shock—verifiable rules reduce information asymmetry; they do not automatically eliminate run games¹². After “Black Thursday,” Maker introduced D3M and other external liquidity modules through governance (Mehrling 2011’s evolution from lender of last resort to “dealer of last resort” in a local on-chain mirror), showing that the protocol side can design limited liquidity corridors, but without unlimited sovereign-credit injection—macro last-resort lending still belongs at the state layer; the protocol layer supplies auditable parallel discipline, not a substitute for the crisis master switch.

New Keynesianism: the welfare foundation of the 2% target. Woodford–Galí models under nominal rigidities and the ELB supply a welfare optimum near a 2% target and FIT—hence fixed collateral parameters can scarcely replicate countercyclical fiscal–monetary coordination; this book accepts FIT within sovereign systems and introduces verifiable constraints only on the dimensions of mint prerogative and issuance discipline. Galí and Galí–Monacelli and other New Keynesian models link a moderate inflation target to nominal rigidities and zero-lower-bound risk¹³; flexible inflation targeting claims already to include the employment gap in the reaction function. If that defense holds, fixed rules or collateral parameters are welfare-inferior to central-bank discretion. Within sovereign fiat systems, FIT remains among best practices; what deserves questioning is whether monopoly mint prerogative is therefore unchallengeable—the 2021–2022 “transitory inflation” misjudgment shows that discretionary frameworks likewise depend on model form and political windows, so the debate shifts to “who can independently verify whether constraints are executed”; Cantillon effects also mean distributional consequences have long been underweighted. The protocol side’s contribution is moving issuance constraints from the conference room onto an on-chain state machine: core PCIM parameters such as collateral ratio C_0 are readable by any third party, so “hidden easing” must occur through visible governance proposals rather than only through footnotes to the central-bank balance sheet. PCIM cannot replicate countercyclical fiscal–monetary coordination; in deep recessions the “pushing on a string” problem exists for protocols too—that is functional division of labor, not theoretical failure.

The refined version of MMT. When floating rates, domestic-currency debt, and a reliable tax base all hold, MMT’s account of tax recovery and Treasury reserve management describes sovereign-layer macro space; it does not automatically imply “protocol money has no place forever.” Sargent–Wallace (1981) show that fiscal deficits paired with low rates may trigger inflationary blowback in the long run—in weak institutional environments, the protocol path’s value is supplying an exitable, verifiable parallel unit-of-account option. Protocols cannot replace redistributive politics and job-guarantee programs. Section 4 already stated MMT’s core proposition; the refined version adds: tax recovers liquidity, Treasuries are a reserve-management tool, and a job guarantee can be fiscally led without traditional financing constraints—under floating rates and domestic-currency debt, the real constraints are inflation and resources, not balances. If MMT’s framework holds, “protocol discipline” may be fighting the wrong problem; the state could properly use monetary sovereignty to serve full employment. The response: MMT’s description of U.S.-style monetary sovereignty has local truth at the level of accounting identities, but cannot be universalized—Turkey, Argentina, Venezuela, and similar cases show that political pressure + thin tax base + capital flight can quickly turn the “inflation constraint” from an abstract curve into a real crisis; MMT policy recommendations lack institutional guardrails replicable in high-inflation democracies. The protocol path does not answer “how to achieve full employment”; it answers “when the fiscal–monetary boundary is eroded, can there exist exitable, verifiable options for pricing and store of value”—

Venezuela's grassroots adoption of stablecoins is a forced test; popularization expands participation and audit, not an automatic welfare state.

Protocols cannot replicate Bagehot-style unlimited injection; Brunnermeier–Niepelt equivalence depends on particular fiscal arrangements and is not automatically satisfied by any on-chain token. Shifting the constraint carrier from institutional reputation to verifiable rules supplies an option, not a full substitute for the macro welfare function or the lender-of-last-resort role—empirical evidence is still needed on on-chain penetration in high-inflation corridors, governance resistance to capture, and peg stress tests; one cannot read “the boundary has been redrawn” from “code exists.”

Section 9. Debt Cycles, Monetary Resets, and Institutional Resilience

In discussions of the fiscal–monetary boundary, one topic is carefully avoided in mainstream policy talk—the top of the debt cycle and the possibility of “reset.” When sovereign debt accumulates to a critical point, conventional fiscal consolidation (tax rises, spending cuts) is politically infeasible, and continued monetization would trigger an inflation spiral; history has repeatedly seen “structural resets”: digesting over-accumulated debt through orderly or disorderly restructuring (default, extension, creditor write-downs), inflationary redistribution of wealth, or fundamental change in the monetary regime (leaving gold, switching exchange-rate regimes).

Contemporary major economies' debt stocks sit at historical highs. The U.S. Congressional Budget Office (CBO) projects federal debt held by the public at about 98% of GDP in fiscal 2024, rising to about 122% by 2034 (*Budget and Economic Outlook*, June 2024); Japan's gross debt-to-GDP was about 255% in 2023 (IMF *WEC* database); euro-area overall government debt-to-GDP was about 88% in 2023, Italy about 137%, France about 110%¹⁴. The 2022–2024 global hiking cycle rapidly raised government interest expense—U.S. Treasury net interest as a share of federal spending rose from about 5% in fiscal 2021 to about 13% in fiscal 2024 (same CBO report)—further compressing fiscal space. Many analysts hold that the scale and speed of this debt accumulation are unsustainable in the long run and that some form of “deleveraging” will eventually occur; normative judgment (“unsustainable”) and positive judgment (“when and how adjustment comes”) must be separated: the former is an inference from fiscal dynamics models; the latter has historically often lagged model warnings (Japan's high debt with low rates is a counterexample)—point forecasts are unwarranted.

This macro background helps explain why “hard asset” narratives gained wide attention in the 2020s—narrative heat is not substitute money already taking over the unit-of-account function. Bitcoin, gold, commodities, even real estate are seen by some investors as hedges for a potential fiat-debt-system reorganization; on-chain reserve assets (including the Bitgold design draft in the Openverse whitepaper) emphasize, on whitepaper terms, value accounting independent of any single sovereign debt table—but Bitgold is a market-priced volatile crypto asset, not sovereign-held foreign-exchange reserves, and cannot equivalently replace a Plano Real-style “exogenous anchor.” Whether it can play a hedge role in systemic crisis depends on: on-chain liquidity depth, availability of fiat on/off ramps under capital controls, and whether PCIM redemption runs remain controllable under high volatility. The gap between possibility (technically holding on-chain assets) and actuality (retail and public finance still priced in domestic currency), like Venezuela's grassroots stablecoin adoption, must be measured with penetration and corridor data, not read straight from a whitepaper roadmap.

The ultimate test of institutional resilience is not whether design looks elegant in calm times, but whether the boundary holds under stress tests, and whether, when it does not hold, substitute mechanisms can take over in time at sufficiently low friction cost. History's answer is plural: independent central banks perform excellently in ordinary environments but cannot stay isolated from political pressure in extremes; international coordination mechanisms supply partial buffers in crises but are often slow and inefficient because of conflicting national

interests; protocol-layer rule constraints supply new design options, yet their true resilience has not yet been historically tested by a sovereign-scale debt crisis—as with CBDC concentrating boundary decisions at the central bank and protocols exposing parameters to on-chain governance, which is easier to capture must be tested case by case, not decided a priori. These options can complement in layers rather than exclude one another; the path of monetary popularization should here be narrowed to: expanding the option space for participation and verifiable constraint, not asserting that protocols have already replaced fiscal–monetary separation.

Loosening and reshaping of the boundary gain new technical expression in CBDC advances. Niepelt’ s 2024 monograph splits the CBDC policy agenda into Whence–Why–What–How: motives from cash decline and the rise of private digital payments; tool choice involving account-/token-based and direct/indirect architectures; and the core tension in the How column is whether programmable retail CBDC can draw a line between “payment infrastructure” and “fiscal targeting tool”¹⁵. Disagreement in the What column is equally critical: account-based CBDC makes every transfer naturally auditable; token-based is closer to cash but AML costs are higher—Niepelt’ s Chapter 4 notes that this choice directly sets the default boundary of privacy and compliance, not a post-hoc patch¹⁶. Fernández-Villaverde, Sanches, Schilling, and Uhlig’ s 2021 working paper formalizes the boundary problem: if retail CBDC allows “central-bank accounts for all,” deposit migration and bank-run risk rise; if CBDC is only for wholesale clearing or strictly capped, it looks more like payment infrastructure than a store-of-value substitute—programmability must therefore be designed jointly with holding permissions, not defaulting to juxtaposing “smart-contract wallets” with “uncapped central-bank liabilities”¹⁷. Targeted subsidies, automatic tax withholding, and crisis consumption vouchers embedded in the same central-bank wallet make monetary neutrality harder to maintain operationally—contrasting with Chapter 10, Section 1’ s “limited constraint on political intervention”: technology can write the boundary into smart contracts, but what is written into contracts may also be the finance ministry’ s execution logic. Bindseil and Panetta’ s 2021 ECB occasional paper approaches the same problem from functional scope: if CBDC’ s functions are too wide, they crowd out private payment innovation; if too narrow, network effects fail—under payment-industry network externalities, the “right width” cannot be judged a priori; control devices such as holding caps, zero remuneration, and reverse waterfall (excess CBDC automatically swept back to bank accounts) must lock CBDC in a medium-of-exchange rather than store-of-value role¹⁸. Bindseil stresses that most central banks deliberately design retail CBDC as non-interest-bearing, holding-capped payment-type liabilities precisely to avoid its becoming a store-of-value asset competing with Treasuries and softening the fiscal–monetary firewall; once CBDC pays interest and caps are lifted, Sargent–Wallace-style “unpleasant monetarist arithmetic”—the central bank forced to accommodate the fisc under high debt—may appear faster on a digital ledger¹⁹. Woodford (1996) supplies the mirror proposition from public-debt dynamics: long-run price stability requires sufficient constraint on the debt stock—if the fiscal path is unsustainable, monetary policy must eventually validate via inflation or default²⁰. Brunnermeier and Niepelt’ s equivalence theorem here supplies a debatable boundary: when CBDC pays interest and has no holding cap, equivalence conditions no longer hold—in high-debt regimes, interest-bearing CBDC and Treasuries form a competitive safe-asset spectrum; if CBDC is strictly locked as payment-type (non-interest-bearing, waterfall, tiered negative rates), equivalence can still hold on paper—Nigeria’ s eNaira low adoption shows a network-effects gulf between intent and landing. This does not assert that CBDC necessarily erodes the boundary; one must see that state and protocol paths form a mirror on boundary auditability—CBDC concentrates boundary decisions at the central bank and legislature; protocols expose parameters to on-chain governance and collateral state; which is easier to capture politically must be tested case by case, not decided a priori.

注释与引用

1. Bank of Japan (BOJ), *Monthly Report of Recent Economic and Financial Developments* and *JGBs Held by the Bank of Japan* statistics: December 2023 holdings about ¥581 trillion, about 52% of issuance; from about ¥164 trillion at QQE launch in April 2013 to about ¥733 trillion balance sheet in 2023 (peak about 132% of nominal GDP; see Chapter 8, Section 7 ⁶). <https://www.boj.or.jp/en/statistics/boj/other/acmai/index.htm> ↩ ↩²
2. Federal Reserve, *Financial Statements and Annual Report* (2023): transfers to Treasury about \$7.6 billion (2023), 2015 peak about \$97 billion; ECB *Annual Report* 2023: remittances about €7.6 billion. https://www.federalreserve.gov/monetarypolicy/bst_fedfinancials.htm ↩
3. Friedman (1970), *Counter-Revolution in Monetary Theory*, Institute of Economic Affairs Occasional Paper 33, p. 24: “Inflation is always and everywhere a monetary phenomenon in the sense that it is and can be produced only by a more rapid increase in the quantity of money than in output.” PDF: https://fraser.stlouisfed.org/files/docs/publications/books/counter_revolution.pdf ↩
4. Fisher (1911), *The Purchasing Power of Money*, around p. 70: increases in the quantity of money are among the most common causes of disturbing equilibrium and “set[ting] up oscillations”; the price level moves with the money quantity. English edition: <https://fraser.stlouisfed.org/title/purchasing-power-money-5379> ↩
5. Fisher (1920), *Stabilizing the Dollar*, ch. 4: “what we need is a gold dollar fixed in purchasing power and therefore variable in weight”; for every 1% deviation of the price index from par, adjust the dollar’s gold content by 1%. Wikisource: https://en.wikisource.org/wiki/Stabilizing_the_Dollar/Chapter_4 ↩
6. QE mechanisms, three rounds of purchases about \$3.7 trillion, distributional consequences, and “correlation ≠ causation” in Chapter 3, Section 2 ¹⁹ and Chapter 9, Section 4 ¹⁴; Federal Reserve H.4.1 Treasury holdings about 24% (2024): <https://www.federalreserve.gov/monetarypolicy/bst.htm> ; ECB *Statistical Bulletin* securities holdings and PSPP/PEPP peak ranges; Bernanke (2015), *The Courage to Act*, chs. 7–9. ↩ ↩² ↩³
7. Friedman and Schwartz (1963), *A Monetary History of the United States*, p. 300: “the contraction is in fact a tragic testimonial to the importance of monetary forces.” Princeton University Press, 1963. ↩
8. IMF *World Economic Outlook* Database (October 2024): Venezuela CPI inflation about 130,060% in 2018 (year-end year-on-year); *Regional Economic Outlook: Western Hemisphere* (2019) discussion of hyperinflation paths. ↩
9. Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*: high-inflation economies (including Venezuela, Argentina, Turkey) show on-chain stablecoin receive intensity well above the global mean; penetration ≠ institutional substitution, to be read against capital controls and domestic-currency circulation share. <https://www.chainalysis.com/blog/2024-geography-of-cryptocurrency-report/> ↩
10. IMF (2022), *Global Financial Stability Report*, October, Chapter 2 “The Crypto Ecosystem and Financial Stability Challenges,” pp. 43–78 (Terra/Luna collapse, algorithmic-stablecoin systemic risk); Catalini, Goren & Shah (2021), MIT Sloan RP: three-way taxonomy of stability mechanisms. <https://www.imf.org/en/Publications/GFSR/Issues/2022/10/11/global-financial-stability-report-october-2022> ↩
11. Bagehot (1873), *Lombard Street*, chs. 2, 7 (lender of last resort); MakerDAO Risk Team (2020-03-12), “Black Thursday Post Mortem”: ETH -30%+ intraday, zero-price auctions, DAI premium; MakerDAO D3M (2021–2022, source: official technical docs, not independently audited); Mehrling, Perry (2011), *The New Lombard Street*, Princeton, ch. 1 (LLR → dealer of last resort); Federal Reserve H.4.1 and FEDS Notes 2023-044 (Terra contagion contrast). Forum: <https://forum.makerdao.com/t/black-thursday-post-mortem/1853> ↩
12. Ahmed, Rashad, Iñaki Aldasoro, and Channele Duley (2024/2025 rev.), “Public information and stablecoin runs,” BIS Working Paper 1164 (reserve-quality disclosure paradox and run coordination; cross-read with Goodhart’s two concepts and Brunnermeier–Niepelt equivalence); Li, Ye, Stephen Meyer, and Andrei Zlate (2023), “Runs and Flights to Safety: Are Stablecoins the New Money Market Funds?,” Federal Reserve Bank of Boston Research Series SRA 2302 (2022–2023 Terra/USDC runs vs MMF-style flight-to-safety). <https://www.bis.org/publ/work1164.htm> ; <https://www.bostonfed.org/publications/research-special/2023/runs-and-flights-to-safety-are-stablecoins-the-new-money-market-funds> ↩
13. Woodford (2003), *Interest and Prices*, chs. 6–7 (nominal rigidities and ELB); Galí (2015), chs. 8, 15 (FIT); Galí & Monacelli (2008), “Optimal Monetary and Fiscal Policy in a Currency Union,” *Journal of International Economics* 76(1), pp. 116–132. ht

[tps://doi.org/10.1016/j.jinteco.2008.08.003](https://doi.org/10.1016/j.jinteco.2008.08.003) ↩

14. CBO (June 2024), *The Budget and Economic Outlook: 2024 to 2034*: federal debt held by the public / GDP about 98% in 2024, about 122% in 2034; net interest / spending about 5% in 2021 → about 13% in 2024. <https://www.cbo.gov/publication/60039> ; IMF *WEO* Database (October 2024): Japan gross debt/GDP about 255% in 2023; euro area about 88%, Italy about 137%, France about 110%. ↩ ↩²
15. Niepelt (2024), *Central Bank Digital Currency: Whence, Why, What, and How*, MIT Press, chs. 1–2 (four-question frame), chs. 5–6 (retail CBDC and fiscal–central-bank division of labor); Bindseil (2024), ECB OP 322, §§5–6 (payment-type vs investment-type CBDC, holding caps): <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op322~5822218919.en.pdf> ↩
16. Niepelt (2024), *Central Bank Digital Currency: Whence, Why, What, and How*, MIT Press, ch. 4 (account- vs token-based CBDC, privacy–compliance default boundary), chs. 5–6 (programmability and fiscal–central-bank division of labor); Brunnermeier & Niepelt (2020), “On the Equivalence of Private and Public Money,” *Journal of Monetary Economics* 106, pp. 27–41 (cases where equivalence fails). <https://mitpress.mit.edu/9780262047555/central-bank-digital-currency/> ; <https://doi.org/10.1016/j.jmoneco.2019.10.006> ↩
17. Fernández-Villaverde, Jesús, Daniel Sanches, Linda Schilling, and Harald Uhlig. “Central bank digital currency: Central banking for all?” *Journal of Monetary Economics* 134, November 2023, pp. 1–15 (orig. NBER WP 26753, 2020; CBDC design spectrum: wholesale vs retail, holding permissions and bank runs; programmability must be bundled with caps). <https://doi.org/10.1016/j.jmoneco.2023.05.004> ; <https://www.nber.org/papers/w26753> ↩
18. Bindseil, Ulrich & Fabio Panetta & Ignacio Terol (2021), “Central Bank Digital Currency: Functional Scope, Pricing and Controls,” ECB Occasional Paper 286, §§2–4 (functional scope, disintermediation, and network effects); Kumhof, Michael & Clare Noone (2021), “Central bank digital currencies — design principles for financial stability,” BIS WP 880, §§3–5 (holding caps and financial-stability design principles). <https://ssrn.com/abstract=3975939> ; <https://www.bis.org/publ/work880.htm> ↩
19. Sargent & Wallace (1981), “Some Unpleasant Monetarist Arithmetic,” *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1981, pp. 1–17: under high deficits, low rates accommodating the fisc must eventually be validated by higher inflation. <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ↩ ↩²
20. Woodford (1996), “Control of the Public Debt: A Requirement for Price Stability?,” *NBER Macroeconomics Annual* 11, pp. 143–169 (public-debt dynamics and price stability; dialogue with Sargent–Wallace 1981); Leeper (1991), “Equilibria under ‘active’ and ‘passive’ monetary and fiscal policies,” *Journal of Monetary Economics* 27(1), pp. 129–147. <https://doi.org/10.1086/654291> ; [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ↩

§ 11 Central Bank Digital Currency and Payment Systems

Tension at the fiscal–monetary boundary takes a new technical form in the advance of central bank digital currency (CBDC); this chapter examines that shock.

When Bitcoin was born in 2009, it pointed straight at pain points in existing payment infrastructure: Why do global transfers take days, several intermediaries, opaque fees, and a permission that any node can deny at any time? More than a decade later, that question reached the community of central banks worldwide. The rise of Central Bank Digital Currency (CBDC) is the traditional monetary system's active response to the digital challenge—an attempt to renew the underlying architecture of payment technology while retaining the core authority of the sovereign monetary system. That renewal will reshape competition in the financial system and continue to contend with the on-chain asset ecosystem. This chapter surveys CBDC's conceptual spectrum, national practices, and the institutional logic behind them.

Section 1. The Layered Structure and Operating Logic of Payment Systems

Any discussion of CBDC must rest on a clear grasp of existing payment systems. Modern payments are highly layered: final settlement relies on central-bank reserves; everyday transactions run through commercial-bank account systems; payment networks (UnionPay, Visa, Mastercard, SWIFT) connect different account systems as upper-layer intermediaries.

The system runs relatively smoothly in advanced economies, but several structural defects remain. **Speed:** domestic retail payments in mobile-payment-advanced countries can settle in seconds, but cross-bank and cross-border payments still depend on batch clearing; T+1 or even T+3 cycles are outdated today. **Cost:** domestic transfer fees in advanced economies have fallen sharply, but the median fee for international remittances remains around 6%, far above acceptable levels; remittance rates in low-income countries are higher still, and those remittances are often an important income source for developing-country households¹. **Inclusion:** about 1.4 billion adults worldwide remain unbanked, without access to basic financial services, concentrated mainly in Sub-Saharan Africa, South Asia, and Southeast Asia¹. **Programmability:** existing payment systems cannot natively support conditionally triggered payments, automatic compliance checks, cross-border asset settlement, and other smart-contract functions; the digital economy's demand for conditional payments and traditional payment infrastructure show a widening rift. Technical roles of payment layering, correspondent banking, and the SWIFT message stack appear in Chapter 8, Section 5; this section only lists the friction inventory that official CBDC narratives target.

“Programmable money” is a pivot concept for the next stage of digital payments. Traditional money is in essence non-programmable: a banknote or a bank transfer carries only amount and payee information and cannot embed any use conditions. Smart-contract money can embed logic: automatically complete payment only after goods arrive at a specified address; embed restrictions: government subsidy vouchers usable only for specified categories of consumption; embed triggers: automatically execute refinancing when rates exceed a threshold. Fisher in *Stabilizing the Dollar* once imagined periodically adjusting the dollar's gold content by a wholesale price index so that the monetary unit would carry computable purchasing power rather than a fixed metal weight²—today's embedded logic of CBDC and on-chain protocols can be read as an extension of that “rules-based money” idea into the digital age. Programmability upgrades money from a single tool of value transfer into a logic layer that can carry complex economic contracts. If CBDC integrates with smart-contract infrastructure, it will produce material efficiency gains in targeted government subsidies, supply-chain finance,

conditional payments, and similar scenes, and will open new tool space at the level of monetary-policy implementation—for example, injecting purpose-specific money directly into particular groups, precisely limiting its use, and bypassing inefficient transmission chains.

CBDC's appearance is cast in official discourse as a technical upgrade solving the problems above—supplying digital cash backed by sovereign credit, bypassing inefficient middle layers, lowering payment costs, and expanding financial inclusion. That positioning should be read as follows: a BIS 2023 survey of 86 central banks found 93% engaged in CBDC work, yet successful cases of large-scale retail replacement of existing account systems remain few³—between technical possibility and institutional landing sit observable bottlenecks such as holding caps, two-tier operation, compliance interfaces, and network effects. Behind official narratives lie more complex strategic considerations: meeting the regulatory challenge of private stablecoins and crypto assets, maintaining monetary sovereignty over payment data, and gaining first-mover advantage in digital-money infrastructure amid geopolitical competition. Whether CBDC can produce statistically significant improvement in remittance costs, unbanked coverage, or cross-border latency must be tested with corridor panels and pilot countries' active-wallet shares; one cannot read “payment monopoly already broken” straight from a whitepaper roadmap.

Section 2. CBDC's Conceptual Spectrum and Classification

CBDC is not a single technical scheme but a broad conceptual framework covering multiple technical architectures and policy-design choices. Distinguish these differences before discussing policy effects.

Wholesale CBDC and retail CBDC are the most basic classification. Wholesale CBDC faces financial institutions, used for interbank clearing and financial-market settlement; in essence it digitally upgrades central-bank reserves and may introduce distributed-ledger technology to raise settlement efficiency. This type has almost no direct effect on the general public; it is mainly a technical update of back-office infrastructure among financial institutions, with relatively limited political controversy. Retail CBDC is the type that sparks broad discussion: it faces individuals and firms directly; any citizen can hold a digital wallet “directly” booked at the central bank, bypassing commercial banks as intermediaries of money holding.

Account-based and token-based are another important dimension. Account-based CBDC resembles a digital bank account at the central bank; transactions require real-name identity verification. Token-based CBDC resembles digital cash, held as electronic tokens, transferable anonymously or semi-anonymously, closer to the functional features of physical cash. The two modes differ sharply in privacy protection, compliance monitoring, and AML/KYC difficulty, and therefore diverge sharply in political acceptability.

Direct, indirect, and hybrid classify operating architectures. Direct CBDC is provided by the central bank to the public; the central bank bears all customer relationships and technical maintenance. Indirect CBDC (also called synthetic CBDC or sCBDC) is provided to the public by authorized intermediaries (commercial banks, payment service providers), backed by fully reserved central-bank liabilities; users actually hold private institutions' liabilities rather than direct claims on the central bank. Hybrid combines the two: the central bank maintains a backup ledger; day-to-day operations are borne by intermediaries. Direct type puts the greatest competitive pressure on commercial banks; indirect type maximally preserves the existing financial architecture; hybrid is a compromise.

Niepelt further aligns the above classifications with policy questions: wholesale CBDC mainly answers whether final settlement must still stack T+1 and correspondent banks; retail CBDC must simultaneously answer whether the public can still convert private deposits at par into public money and whether non-banks can access central-bank liabilities⁴. His 2024 *Journal of Finance* paper then asks about architecture choice: when banks

have market power on the deposit side, optimal CBDC and reserve rates should differentiate, and CBDC's optimal share in payments may be higher than deposits—unless the social cost of central-bank refinancing to banks is too high⁵. The BIS 2020 seven-central-bank principles and Bindseil's 2024 survey both stress two-tier operation (central bank issues, private institutions reach users) as the default preference—not a technical necessity, but a way to keep disintermediation risk in an acceptable range: user wallets are maintained by banks or payment institutions; central-bank liabilities remain on the balance sheet, paired with holding caps discussed in Section 4. The BIS 2021 system-design and interoperability report further clarifies engineering constraints: identity, wallet, and ledger layers must separately connect to existing RTGS and card schemes; retail CBDC is an incremental module, not an overnight replacement of the wholesale stack⁶. China's e-CNY two-tier architecture and the “waterfall mechanism” in ECB legislative drafts (excess CBDC automatically swept back to the bank end) institutionalize this approach. On-chain protocol readers easily take “bypassing banks” as pure technical gain; academic dialogue reminds us that which layer is bypassed—the retail interface, credit creation, or central-bank final settlement—has sharply different consequences.

Section 3. Major CBDC Practices Worldwide

As of 2026, more than 130 countries are researching, piloting, or launching CBDC to varying degrees, covering over 95% of global GDP. The BIS 2023 survey of 86 central banks shows 93% engaged in CBDC work, more than half in pilot or advanced development—a share unimaginable when the BIS issued its first joint-principles report in 2020³. Boar, Holden, and Wadsworth's 2021 prior survey of the same cohort already showed an inflection: about 86% of central banks in active research or experiment, 60% running proofs of concept or pilots—CBDC shifted rapidly from “whether” to “how”⁶. Several representative practices deserve deeper analysis.

China's e-CNY is to date the largest and most mature retail CBDC deployment. The People's Bank of China began research in 2014 and launched a series of pilots from 2020 in Shenzhen, Shanghai, Beijing, and other major cities. e-CNY adopts a two-tier operating architecture: the PBOC issues; commercial banks and some payment institutions operate, providing digital wallets and everyday payment services to the public. The technical design is “controllable anonymity”—small amounts anonymous (protecting personal privacy), large amounts real-name (meeting AML requirements). e-CNY is explicitly positioned as a digital form of cash, pays no interest, and mainly aims to raise retail payment efficiency, lower cash-management costs, and, at a deeper level, strengthen control over cross-border payment data.

The Bahamas Sand Dollar, formally launched in October 2020, was among the world's earliest fully launched national retail CBDCs. Its background is the Bahamas' archipelagic geography: dispersed islands make physical cash distribution costly; many residents (especially on remote islands) lack banking services. The Sand Dollar is accessible via mobile phone, lowering the threshold for financial services—a classic case of CBDC as an inclusion tool. Limited by the Bahamas' economic scale, its systemic impact is relatively limited.

The ECB's digital euro project has progressed relatively cautiously. The ECB began a two-year investigation phase in 2021, entered preparation in 2023, and is not expected to reach actual deployment before 2027–2028. European concerns about CBDC concentrate on two points: impact on the commercial-banking system, and privacy (European public expectations for financial-data privacy are far higher than in Asia; government control of payment data is viewed with high vigilance). Digital-euro design principles explicitly include offline payment capability (no network needed, closer to cash) and holding caps (preventing excessive deposit substitution).

Nigeria's eNaira, launched in October 2021, was Africa's first national CBDC. Adoption has been disappointing: an IMF 2022 country report citing central-bank data shows about 8.4 million cumulative wallet

registrations by August 2022, but monthly active transaction counts long stayed low—the IMF estimates the share of population in actual daily use on the order of about 0.5%, far below mobile payments and dollar stablecoins locally⁷. Causes include lack of use cases, technical instability, and mismatch with existing mobile-payment habits. The case supplies an important warning: between government’s capacity to launch CBDC and the market’s willingness to adopt lies an observable gulf; technology-first deployment without real use cases and user incentives tends toward idle fate.

eNaira’s failure is not unique; it reflects a basic law of monetary economics: money’s value comes from wide use; to be widely adopted, users must first believe others will also adopt. Fernández-Villaverde and Sanches (2019) in the *International Economic Review* formalize this coordination dilemma: a new payment medium must cross a critical network size—before the threshold, private adoption incentives are insufficient; if government cannot supply a strong enough initial anchor (tax, subsidy, compulsory settlement), CBDC can long remain in a “registered but unused” equilibrium⁸. That does not contradict Keister and Monnet’s more optimistic conclusion that CBDC reduces normal maturity mismatch: the latter discusses financial stability *after* adoption; the former discusses *whether* adoption occurs—Nigeria’s eNaira is stuck at the latter. Government can push initial adoption by compulsion (e.g. taxes paid in CBDC) or incentive (e.g. subsidies disbursed via CBDC), but the degree of compulsion determines how “real” CBDC penetration is. Digital payment tools that truly gained mass use in Nigeria have often been mobile apps and dollar stablecoins that solve users’ real pain points, not policy-driven CBDC—eNaira’s lesson: without real scenes and incentives, technical deployment alone does not buy adoption. Observable contrasts include: pilot-country CBDC active wallets as a share of M2 or adult population; whether corridor remittance costs fall significantly because of CBDC; whether on-chain stablecoin receive intensity in high-friction economies is systematically higher than CBDC penetration—if any of the three fails to improve, the claim “CBDC has rewritten the payment monopoly” is unsupported; only “the sovereign is experimenting” is supported.

Section 4. CBDC’s Impact on the Commercial-Banking System

Retail CBDC’s most contested policy effect is structural impact on the existing commercial-banking system. In the current system, personal savings are held as deposits at commercial banks; banks use those deposits as funding and, through credit creation, lend to households and firms—the economy’s primary credit intermediaries. If retail CBDC is convenient to use, free of credit risk (central-bank liabilities have no commercial-bank failure counterparty risk), and offers competitive store-of-value features, large-scale migration of funds from bank deposits to CBDC wallets becomes a reasonable expectation.

This deposit disintermediation risk can be described numerically at stress-test magnitude (not a forecast): if only 5% of China’s household deposits migrated to e-CNY, then on PBOC 2024 financial-institutions credit-receipts-and-payments household deposits of about RMB 150 trillion, about RMB 7.5 trillion would be involved; if some corporate demand deposits are included, the order of magnitude can approach RMB 12 trillion—this book takes the latter as a tail-scenario illustration⁹. Contraction of the deposit base would directly compress banks’ lending capacity, possibly triggering credit contraction and higher rates, contrary to CBDC’s original aim of raising payment efficiency. Fisher already stressed in 1911 that check deposits and coin jointly constitute the circulating medium; deposit migration changes the entire credit-creation structure, not merely payment technology¹⁰. For smaller banks, deposit disintermediation may trigger liquidity crisis and then systemic financial risk.

In a financial crisis, CBDC’s deposit-disintermediation effect may amplify sharply, forming new systemic fragility. If public confidence in commercial banks falls, the incentive to hold CBDC (credit-risk-free central-bank

direct liabilities) rather than bank deposits (with counterparty risk) can surge, potentially triggering an extreme “digital bank run.” Keister and Monnet’s model reminds us that this concern is correct in direction, unsettled in net effect—CBDC availability reduces banks’ normal maturity mismatch, partly offsetting run exposure; but instant migration of funds to CBDC in crisis can still serve as a signal of weak banks, shortening the supervisory response window¹¹. In traditional banking, withdrawals are constrained by physical conditions (ATM networks, business hours, counter queues), objectively buffering the speed of panic transmission. If CBDC is provided as a mobile app, funds can move in seconds; panic transmission is orders of magnitude faster than traditional runs, and the time for systemic pressure to accumulate shrinks sharply—unless holding caps, waterfall mechanisms, and tiered remuneration make CBDC inferior to bank deposits at the margin, “digital run” tail risk must be modeled separately in stress tests¹². This is a systemic-risk dimension of CBDC design not yet fully researched; central banks designing holding caps and technical architecture need to bring this scenario into stress-test frameworks rather than leave it for future crises to test.

Central banks have designed various “anti-disintermediation” mechanisms against this risk: caps on individual CBDC holdings (the ECB proposes €3,000 per person; early e-CNY pilots set similar limits); paying no interest on CBDC (reducing its attraction as a store of value); under indirect architectures, ensuring commercial banks remain the user interface (preserving customer relationships and some profit sources). These measures to some extent weaken CBDC’s potential benefits, yet are necessary compromises for financial-system stability.

Bindseil and Auer et al.’s survey of the disintermediation literature notes that shock size depends heavily on whether CBDC resembles cash or deposits—if interest-bearing and uncapped, some models show euro-area CBDC as a share of broad money reaching double digits; if non-interest-bearing with a per-person cap of about €3,000, total absorption is on the order of €1 trillion, with possibly limited marginal effects on bank net interest margins and credit supply, but higher crisis-tail sensitivity to holding caps and rate design¹². Brunnermeier, James, and Landau’s work on “the digitalization of money” adds a platform dimension: when large tech platforms bundle payments, data, and credit, bank liabilities may be eroded not only by CBDC but by “in-platform closed-loop money”; retail CBDC is here envisioned as a public option to maintain unit-of-account unity and monetary sovereignty—forming triangular competition with private stablecoins and on-chain public-domain money (VRC-10) for the “default dollar” in emerging markets, not a simple “state vs crypto” binary.

The deeper question: in the macro-policy framework, are CBDC and the commercial-banking system complements or substitute competitors? If the central bank decides to provide uncapped CBDC deposits to the public and pay interest on them, the central bank in substance becomes a giant “commercial bank,” squeezing private banking and changing the whole financial system’s credit-allocation mechanism—Sargent and Wallace’s (1981) unpleasant monetarist arithmetic may appear faster in this scenario: in high-debt regimes, interest-bearing CBDC attracts the public to hold central-bank liabilities, fiscal financing pressure rises, and the central bank is forced to accommodate with inflation¹³. Leeper (1991) and Woodford (1996) formalize the same logic: under “active fiscal, passive monetary” equilibria, public-debt expansion is more likely to be validated by a rising price level than by tax adjustment—interest-bearing, uncapped retail CBDC amounts to writing unpleasant arithmetic onto the digital ledger¹⁴. This is the outcome most CBDC designers explicitly try to avoid, but “what counts as enough complement rather than excessive substitute” has no clear technical boundary.

Section 5. The Regulatory Logic of Payment Licenses and the Interest Landscape

Access qualifications for payment systems are strictly regulated. Obtaining a payment license means being allowed to provide customers with money-movement services; this entry barrier takes different forms in different countries: U.S. money-services business (MSB) licenses, China’s payment-business permits, EU payment

institution (PI) and electronic-money institution (EMI) licenses. These permits are not only legal requirements of regulatory compliance but also critical moats of market competition.

The official logic of payment licensing is: payment systems carry massive fund flows; once a payment provider fails or mismanages, customer funds face loss risk and systemic financial risk may spread. Strict capital requirements, reserve-management rules, operating standards, and periodic audits aim to ensure licensed institutions have sufficient financial soundness and compliance capacity. From this angle, payment licensing is a necessary institutional design for financial consumer protection and system stability. Friedman, discussing the roots of inflation, noted that only government monopoly of the central bank and the printing press can create monetary expansion beyond output; firms and households lack that power¹⁵—payment-access licensing, in a sense, extends the state’s monopoly control over money creation and transfer channels.

Yet payment licensing is also a protective device for the existing interest landscape. Licensed large banks and payment institutions have built complex compliance infrastructure over years and can easily clear entry hurdles; startups and nontraditional actors entering the payment market face compliance investment and approval cycles that form substantial barriers to entry. National regulators generally show caution or even resistance when issuing payment licenses to crypto-asset firms; the official reason is AML/CFT risk, but critics note that this caution also conveniently protects traditional financial institutions from competitive shock. Historically, every major technical change in financial services has been accompanied by lagged adaptation of the regulatory framework: credit cards, ATMs, internet banking, mobile payments—all without exception moved from regulatory confusion to gradual normalization, eventually finding institutional equilibrium in competition. Crypto payment protocols are in the early stage of this adaptation; the ending is unpredictable, but the direction is more likely finer licensing than total blockade.

As CBDC advances, the payment-license landscape is being reshaped. On one hand, indirect CBDC architectures require that non-bank payment institutions can also become authorized operators, partly opening channels for non-banks into core payment rails; on the other, CBDC launch may further strengthen scrutiny standards for access institutions on “systemic importance” grounds, forming higher thresholds. Stablecoin issuers and crypto payment platforms face rising compliance pressure in multiple major jurisdictions; regulatory-arbitrage space is narrowing. For blockchain payment protocols, obtaining payment-system access within bearable compliance cost is a necessary gate from technical experiment to real scaled deployment.

Section 6. Intersection and Tension Between On-Chain Assets and CBDC

CBDC and on-chain assets (including stablecoins, native tokens, and tokenized real-world assets) do not evolve in two parallel universes. They collide at multiple functional junctions—payment settlement, asset custody, and currency conversion—with both collaborative possibilities and deep institutional competition.

In cross-border payments and settlement, CBDC and on-chain stablecoin paths may converge. The BIS-led mBridge project (a multilateral wholesale CBDC platform involving the Hong Kong, Thai, UAE, and Mainland Chinese central banks, among others) entered a minimum viable product phase in 2024 after a 2022 proof of concept: multiple countries’ CBDCs perform PvP (payment-versus-payment) atomic settlement on the same distributed ledger, aiming to compress cross-border payments from days to seconds and reduce dependence on correspondent networks¹⁶. Project Dunbar (Australian, Malaysian, Singaporean, and South African central banks, 2022 PoC) and Project Aber (Saudi and UAE dual-central-bank wholesale CBDC, 2020 PoC) supply complementary samples: Dunbar validates shared clearing logic under a multi-CBDC platform; Aber validates cross-border PvP by dual issuers on the same ledger—together with mBridge they show that sovereign paths’ interoperability experiments at the wholesale layer lead the retail layer by years⁶. The BIS 2023 *Future of the*

Monetary System report lists this alongside tokenized deposits and unified ledgers as three main lines of “next-generation financial infrastructure”—wholesale CBDC handles final settlement among central banks; on-chain stablecoins handle permissionless retail cross-border; the two overlap functionally in “remittance and trade settlement,” but diverge on compliance and sovereign control. Niepelt warns that allowing non-residents to hold domestic retail CBDC may introduce new channels for cross-border arbitrage and exchange-rate transmission; mBridge’ s choice of the wholesale layer keeps spillovers within the interbank sphere. Bahaji and Prat’ s ECB research on cross-border payments further notes that CBDC–stablecoin corridor competition turns less on technical speed itself than on whether compliance interfaces and FX liquidity close—if on-chain assets cannot connect to wholesale CBDC hubs, they must still “land” via bank gateways¹⁷. For VRC-10 and similar protocols, mBridge is not a direct competitor but a reference for standardizing the sovereign clearing layer: if interoperability interfaces are closed, on-chain assets must still land through banks or compliance gateways; if APIs open, protocol settlement may coexist with wholesale CBDC hubs—depending on whether regulation accepts “on-chain state as final settlement,” still to be tested by regulatory and judicial practice.

In tokenized-asset settlement, wholesale CBDC is seen as the most promising atomic settlement medium. Once bonds, equities, real estate, and other real assets are tokenized, settlement theoretically needs a monetary form that runs on the same digital rail as the tokenized assets to complete delivery-versus-payment. If traditional bank transfers are used, settlement still occurs across two separate systems and friction remains. If wholesale CBDC interoperates with tokenized-asset platforms, true instant atomic settlement becomes possible, eliminating counterparty risk. This application scene is logically promising and is a direction actively pursued by major financial centers.

Tension exists mainly at the retail layer. On-chain stablecoins (especially dollar stablecoins) already provide convenient digital-dollar holding and transfer services to millions of users worldwide, especially in emerging markets with strong dollarization tendencies—Chainalysis’ s *2024 Geography Report* shows Argentina, Turkey, and other high-inflation economies with on-chain stablecoin receive intensity well above the global mean, yet penetration still far below everyday retail fiat¹⁸, a technically feasible fragment, not sufficient evidence that “private dollars have replaced domestic currency.” If CBDC forcibly replaces private stablecoins that already have network effects on grounds of defending monetary sovereignty, it may trigger fierce regulatory–market conflict. Friedman and Schwartz’ s historical research shows that when monetary authorities fail to prevent sharp contraction of the money stock, real recession often deepens¹⁹—if retail CBDC triggers deposit disintermediation and credit contraction, its macro consequences are not essentially different from the path the quantity theory of money warns against. On the other side, VRC-10 (Bitcurrency, public-domain money standard; PCIM competitively issued with Bitgold dynamic-tier overcollateralization (circulation-triggered referenda, upper tier about 161.8%, $C_0 > 100\%$)) and the VRC-11 private-domain layer must be stratified (parameters in the glossary); Openverse and similar protocols, on whitepaper terms, keep functional independence from any sovereign CBDC—issuance rules readable on-chain, decoupled from political power; whether they coexist with CBDC in interoperability and compete with sovereign money in narrative awaits mainnet scale and regulatory precedents, and should not be cast as an oppositional ending straight from a whitepaper. How this competitive landscape evolves will largely shape the digital-money ecosystem’ s map over the next decade—possibility must be tested with penetration, corridor costs, and compliance-interface coverage, not fixed a priori.

Section 7. Regulatory Contests and the Reordering of Monetary Order

CBDC’ s advance is not only a payment-technology upgrade but a deep contest over future monetary-order leadership. Participants include: national central banks (seeking to maintain sovereign-money status), commercial

banks (seeking to protect deposit bases and payment profits), tech firms and payment platforms (seeking to convert technical advantage into access rights to the monetary system), and on-chain protocol communities (seeking to challenge permissioned access systems with open standards).

From a geopolitical dimension, CBDC competition is evolving into a national version of the digital-money standards contest. The dollar system's global dominance rests to a considerable degree on the SWIFT message network and U.S. financial institutions' control of correspondent networks—SWIFT's technical position and message-RTGS layering (see Chapter 8, Section 5); Western countries' 2022 SWIFT restrictions on some Russian banks showed that this infrastructure can be mobilized as a geopolitical tool, and also pushed more countries to assess diversification of payment infrastructure—this is an observable event, not proof that the dollar clearing system has already been replaced. Brunnermeier and Landau's 2022 digital-euro study commissioned by the European Parliament operationalizes monetary sovereignty as: in domestic contracts and retail payments, the unit of account and final settlement remain anchored by domestic public money, not implicitly replaced by global stablecoins or foreign platform money²⁰. Cross-border promotion of e-CNY is read by some analysts as potential infrastructure that may bypass the dollar clearing system—wholesale CBDC experiments such as mBridge have shown technical possibility of second-level PvP, but retail-layer share, non-resident holding rules, and FX liquidity interfaces still determine actual spillovers; if the EU digital euro achieves scaled deployment within the euro area, on whitepaper terms it could strengthen the euro's de facto monopoly in member payment systems. These deployment logics if realized may reshape the global monetary pattern of “dollarization” at the technical level—until then, they should be read as sovereign experimentation and standards competition, not completed order reordering.

Blockchain payment protocols' distinctive geopolitical attribute is that their design itself belongs to no sovereign state. Bitcoin nodes are distributed within countries and each subject to territorial law, but their accounting and clearing rules do not depend on any single jurisdiction's licensed clearing infrastructure—no country's node enjoys a privilege to veto network-wide transactions; stablecoin transfers on Ethereum likewise need no clearing node approved by any state. VTP (Value Transfer Protocol), on the Openverse roadmap, pursues on whitepaper terms decoupling of value-transfer paths from any single country's financial infrastructure—whether it is realized, and whether “landing” is still required before compliance gateways, awaits interoperability tests and regulatory precedents. This denationalized neutrality is both a source of political attraction and the greatest resistance it faces in major countries' regulatory frameworks: no major country is willing to accept a monetary order in which it “cannot sanction other countries through the payment system”—because that means abandoning an extremely effective foreign-policy tool.

CBDC advance gives on-chain protocol communities two simultaneous pulls: large-scale sovereign experimentation on ledgers, contracts, and cross-border wholesale rails supplies a comparable reference for open standards; if the retail layer squeezes private stablecoins that already have network effects by compulsory means, it directly compresses on-chain protocols' operating space. Whether the two tracks can coexist at interoperability interfaces depends on whether regulation accepts “on-chain state as final settlement”—Section 6's contrast of mBridge and VRC-10 is a concretization of that interface question.

Section 8. The Privacy Dilemma and Design Boundaries of Digital Cash

Among all CBDC policy discussions, privacy is the dimension of highest public concern and most intractable institutional design. A rarely stated but widely cherished property of physical cash is its anonymity: when you buy anything with cash, the merchant knows only how much was received, not who you are; the bank does not know your purchasing habits; the government does not know your consumption records. That anonymity is a

deliberately retained social function, not a technical bug—it protects individuals from discrimination based on consumption preferences, protects political dissenters from being tracked by donation records, and protects ordinary citizens from ubiquitous financial surveillance.

If retail CBDC is deployed in an account-based design requiring full real-name identity authentication, the central bank (or its authorized institutions) will hold every transaction record: when, where, to whom, how much. Technically, this is unprecedented financial-surveillance capacity. Supporters argue it can greatly raise AML and CFT efficiency and reduce tax evasion, corruption, and illicit transactions; critics note that any large-scale database held by government may be abused—whether for commercial data analysis, tracking political dissent, or future administrations using it to suppress opposition. The disagreement falls at the level of political institutions; technology itself cannot guarantee that power will not be abused.

In the EU’ s digital-euro design, “protecting payment privacy” is explicitly listed as a core design principle, and offline payment schemes based on hardware secure elements are explored (users hold CBDC balances on local devices; offline transfers need no network verification, achieving near-cash privacy protection). Bindseil and Panetta’ s 2021 occasional paper calls this design tiered privacy: small offline amounts anonymous, large online amounts auditable—alongside holding caps and waterfall mechanisms in digital-euro legislative drafts as “control devices,” aiming to draw a line between AML and cash-like anonymity rather than all-or-nothing²¹. Auer, Cornelli, and Frost in a BIS quarterly survey remind that the default state of account-based retail CBDC is fully chain-traceable—if legislation does not clearly provide offline/token options, privacy protection will be weaker than cash and far stronger than bank secrecy for deposits²¹. The scheme is technically feasible but faces challenges at the compliance-supervision layer: if offline payments are fully anonymous, they bypass AML/KYC requirements, and regulators are highly alert. Finding an acceptable balance between privacy protection and compliance monitoring is among the hardest political-technical problems in CBDC design.

On-chain privacy protocols (such as Zcash’ s zk-SNARKs, Monero’ s ring signatures, and Ethereum Layer-2 privacy applications) offer another approach: cryptographically protect transaction privacy while, when necessary, allowing authorized parties (regulators, court orders) to selectively disclose specific transaction information. This “optional disclosure” design tries to draw a finer boundary between personal privacy and lawful supervision. Whether governments accept it depends on whether power is willing to accept cryptographic constraints—a political choice, not a technical one. The tug-of-war between privacy rights and regulatory transparency will be a main line of digital-money policy debate over the next decade; the equilibrium can only emerge slowly through repeated contests among legislation, technology, and civil society, and will not be fixed unilaterally by any single side.

注释与引用

1. World Bank (2022), *Global Findex Database 2021*: about 1.4 billion adults still unbanked; World Bank (2023), *Remittance Prices Worldwide Q3 2023*: global average remittance cost about 6.2%, Sub-Saharan Africa corridors often above 8% (same metrics as Chapter 8, Section 5¹¹). <https://www.worldbank.org/en/publication/globalfindex> ; <https://remittanceprices.worldbank.org/> ↩ ↩²
2. Fisher (1920), *Stabilizing the Dollar*, ch. 4: “what we need is a gold dollar fixed in purchasing power and therefore variable in weight”; using the index number as a rule “for every one per cent of deviation of the index number above or below par ... increase or decrease the dollar’ s weight by one per cent.” Wikisource: https://en.wikisource.org/wiki/Stabilizing_the_Dollar/Chapter_4 ↩

3. Bank for International Settlements (2023), "CBDCs: Progress and ongoing work," *BIS Papers* No. 125, July 2023, §§1–2 (survey of 86 central banks, 93% engaged in CBDC work): <https://www.bis.org/publ/bppdf/bispap125.htm> ↩ ↗²
4. Niepelt (2024), *CBDC: Whence, Why, What, and How*, MIT Press, ch. 2 (taxonomy and architecture), ch. 4 (two-tier operation); BIS et al. (2020), *Foundational Principles and Core Features*, Principle 3 (coexistence with existing systems): <https://www.bis.org/publ/othp33.htm> ↩
5. Niepelt (2024), "Money and Banking with Reserves and CBDC," *Journal of Finance* 79(4), pp. 2505–2552 (optimal architecture, CBDC payment share): <https://www.niepelt.ch/files/jf2024.pre.pdf> ↩
6. Group of Central Banks and BIS (2021), *Central bank digital currencies: system design and interoperability*, §§2–3 (three-layer architecture and coexistence principles); Boar, Holden & Wadsworth (2021), "Ready, steady, go?," *BIS Papers* No. 114, §§1–2 (86% of central banks actively researching, 60% in pilot/PoC); BIS Innovation Hub, "Project Dunbar" (2022 PoC); "Project Aber" (2020 PoC). <https://www.bis.org/publ/othp38.htm> ; <https://www.bis.org/publ/bppdf/bispap114.htm> ; <https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm> ; <https://www.bis.org/about/bisih/topics/cbdc/aber.htm> ↩ ↗² ↗³
7. IMF (2022), *Nigeria: 2022 Article IV Consultation*, Staff Report, §§4–5 (eNaira wallet registration and low active adoption); KPMG Nigeria (2022), *eNaira: A Diagnostic of Adoption* (monthly active transactions and merchant onboarding bottlenecks). <https://www.imf.org/en/Publications/CR/Issues/2022/11/07/Nigeria-2022-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-the-525000> ↩
8. Fernández-Villaverde, Jesús, and Daniel Sanches. "Can Currency Competition Work?" *Journal of Monetary Economics* 102, November 2019, pp. 1–15 (payment-medium network effects, critical mass, and government initial anchors; formal contrast for eNaira's low adoption). <https://doi.org/10.1016/j.jmoneco.2018.08.004> ↩
9. People's Bank of China, *Financial Institutions Credit Receipts and Payments Statistics*, December 2024: household deposit balance about RMB 151.2 trillion; 5% migration about RMB 7.6 trillion; if quickly migratable demand deposits of non-financial firms are included, tail stress tests can approach RMB 12 trillion—this book takes the latter as illustration, not a point forecast. <http://www.pbc.gov.cn/> ↩
10. Fisher (1911), *The Purchasing Power of Money*, ch. 2: check deposits "even more than money do actually serve as a medium of exchange"; deposits account for about four-fifths or more of the circulating medium in statistics. English edition: <https://fraser.stlouisfed.org/title/purchasing-power-money-5379> ↩
11. Keister & Monnet (2022), "Central Bank Digital Currency: Stability and Information," *Journal of Economic Dynamics and Control* 142, 104501 (OFR WP 22-04, §§1–2, §4.1: CBDC inflows as run signals): https://www.financialresearch.gov/working-papers/files/OFRwp-22-04_central-bank-digital-currency.pdf ↩ ↗²
12. Bindseil (2024), ECB OP 322, §§7–9 (disintermediation and holding caps); Auer, Cornelli & Frost (2022), "CBDC and financial stability," *BIS Quarterly Review*, March 2022, pp. 55–68; Brunnermeier, James & Landau (2019), "The digitalization of money," NBER WP 26300 / BIS WP 941, §5.2 (digital dollarization and CBDC responses): <https://www.bis.org/publ/work941.pdf> ↩ ↗²
13. Sargent & Wallace (1981), "Some Unpleasant Monetarist Arithmetic," Fall 1981, pp. 1–17; Bindseil (2024), ECB OP 322, §§5–6 (payment-type vs investment-type CBDC, holding caps to maintain the fiscal-monetary firewall). <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ↩
14. Leeper (1991), "Equilibria under 'active' and 'passive' monetary and fiscal policies," *Journal of Monetary Economics* 27(1), pp. 129–147; Woodford (1996), "Control of the Public Debt: A Requirement for Price Stability?," *NBER Macroeconomics Annual* 11, pp. 143–169 (jointly with Sargent & Wallace 1981 unpleasant arithmetic; interest-bearing uncapped CBDC scenarios). [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ; <https://doi.org/10.1086/654291> ↩
15. Friedman (1974), BBC *Controversy* lecture "Inflation Is Created by Government and by No One Else": "Only Government has a monopoly of the printing press ... Inflation is always and everywhere a monetary phenomenon." Hoover Institution archive (original transcript, browser-accessible): <https://miltonfriedman.hoover.org/internal/media/dispatcher/271092/full> ↩
16. BIS (2023), *The Future Monetary System* (Annual Economic Report, Chapter III), §§III.B–III.C (mBridge, tokenization, and unified ledgers); BIS Innovation Hub, "Project mBridge: Connecting economies through CBDC," 2024 update (MVP stage): https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm ↩
17. Bahaji, Hamza, and Fabio Prat. "Stablecoins, Central Bank Digital Currencies and Cross-Border Payments." ECB Working Paper 2544, November 2021, pp. 1–45 (CBDC/stablecoin competition and FX liquidity on cross-border corridors). <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2544~7dd2cc491a.en.pdf> ↩

18. Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*: Argentina, Turkey, Nigeria, and other high-inflation/high-friction economies show on-chain stablecoin receive intensity above the global mean, yet share of everyday retail payments remains limited (same citation as Chapter 9, Section 8¹⁸). <https://www.chainalysis.com/blog/2024-geography-of-cryptocurrency-report/> ↩ ↩²
19. Friedman and Schwartz (1963), *A Monetary History of the United States*, pp. 300–301: different and feasible monetary-policy actions could have prevented the decline in the money stock and “would have reduced the contraction’ s severity and almost as certainly its duration.” Princeton University Press, 1963. ↩
20. Brunnermeier & Landau (2022), “The digital euro: policy implications and perspectives,” study for the European Parliament ECON Committee, §§2–3 (public monetary anchor and monetary sovereignty): [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733783/IPOL_STU\(2022\)733783_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733783/IPOL_STU(2022)733783_EN.pdf) ↩
21. Bindseil, Panetta & Terol (2021), ECB OP 286, §§3–4 (tiered privacy, functional scope); Auer, Cornelli & Frost (2022), “CBDC and financial stability,” *BIS Quarterly Review*, March 2022, pp. 55–68 (default traceability of account-based CBDC). <https://ssrn.com/abstract=3975939> ; https://www.bis.org/publ/qtrpdf/r_qt2203e.htm ↩ ↩²

Part IV: Transformation by Protocol

§ 12 Bitcoin and the Battle of Standards

Central-bank monopoly and CBDC experiments provide a foil for on-chain money¹; the on-chain ecosystem that begins with Bitcoin pushes the question back to issuance rules, standard interfaces, and composable design. The “battle of standards” is not only a contest of protocol versions; it is a political-economy question of who defines money, how it is constrained, and in what way it is accepted by global holders—its outcome will deeply shape the practical path of monetary popularization.

Section 1. Intellectual Lineage of the Bitcoin Standard

The Bitcoin Improvement Proposal (BIP) process shows how standards evolve without a central authority: anyone may submit a BIP; miners and full nodes “vote” by whether they upgrade software. Adoption of BIP-141 (SegWit, 2017) and BIP-341 (Taproot, 2021) are verifiable cases of “standards contests” at the protocol layer.

Bitcoin was never an idea from nowhere. Satoshi Nakamoto’s whitepaper of October 2008 took up a core problem economic thinkers had posed but not solved over two centuries: how, without a trusted intermediary, to ensure that money issuance follows predetermined rules and cannot be arbitrarily changed by any actor with political power.

Ricardo’s metallism offered an early answer: constrain money supply by the physical cost of gold extraction, separating political power from determination of the money quantity. Yet the gold standard had historical limits—gold output is governed by geological randomness and cannot flexibly answer cyclical demand; cross-border settlement required physical gold shipment at high friction cost; more fundamentally, maintaining the gold standard depended on governments’ political will to honor convertibility under pressure, and political will historically never withstood sustained stress.

Hayek in *Denationalization of Money* pushed the problem one step further: rather than rely on gold, rely on competitive pressure among private issuers to maintain monetary quality. Competition’s virtue is that it requires no issuer to sustain perfect moral self-discipline; it need only ensure that market participants can identify and choose more stable money; the pressure of voting with one’s feet then forces issuers to keep discipline. But Hayek conceded that the mechanism was hard to sustain under 1976 technical conditions: there was no instant trustworthy information on monetary quality, no low-cost infrastructure for switching currencies, and no issuance record fair and transparent to cross-border holders alike.

Bitcoin answered this old question with an engineering method Hayek had not imagined: cryptographic commitment replaces metallic physical scarcity; a global distributed node network replaces trust in an issuing institution; open-source, public issuance code replaces reserve statements that are hard to audit after the fact. Anyone need not first trust some issuer; they may run a node themselves and check whether every on-chain transaction and the current total supply match the issuance schedule set in code. Monetary trust thus shifts toward verifiable rule execution—in the age of public on-chain ledgers, that shift has sharp institutional meaning, yet should not be exaggerated as a historical singularity: as bookkeeping technology changes, so does what trust attaches to. The second classical premise discussed in Chapter 7—that rule changes must pass auditable procedures—has verifiable instances in the BIP process: SegWit and Taproot adoption rates and full-node version distributions can be checked off-chain; yet the power structure among miners, developers, and holders remains a governance question for research—technical verifiability is not political neutrality.

Section 2. Algorithmic Constraint and Missing Elasticity

Bitcoin's monetary policy is among the most watched and most contested designs in its code. Roughly every four years (more precisely every 210,000 blocks), the block subsidy halves: from the initial 50 bitcoin, to 12.5, to 6.25, to 3.125 after the fourth halving in April 2024. Over time new supply approaches zero; the total cap is about 21 million coins; around 2140 miners are expected to receive no further block subsidy, and network security will then depend on fee income.

This mechanism gives Bitcoin a strong "disinflation narrative"—in an age of long-run central-bank balance-sheet expansion, an asset whose supply curve is fully fixed and alterable by no political force has natural appeal. After subsidy halvings, miner incentives rely increasingly on the fee market—Easley, O'Hara & Basu (2024) use on-chain data to depict this evolution from "mining subsidy" to "market-priced settlement," aligned with Nakamoto's whitepaper §6 fee design². Background on unconventional easing appears in Chapter 3, Section 2³. Against that macro backdrop, Bitcoin's "digital gold" narrative attracted institutional allocation interest: Grayscale trusts, MicroStrategy, and others held long-term; Tesla bought about \$1.5 billion of bitcoin in 2021 and sold most of the position in 2022—institutional narrative is not equivalent to sustained strategic allocation⁴.

Yet the virtue of algorithmic constraint is precisely also its limit. Money in the modern economy is asked to perform three functions: store of value, medium of exchange, and unit of account. Gold's historical record as a store of value is strong, but precisely because of supply rigidity, gold-standard economies could not sustain employment and output through credit expansion in contractions—one lesson of the Great Depression is how gold-standard deflationary forces amplified a local financial crisis into a global catastrophe. Keynes in *A Tract on Monetary Reform* (1923) already called the gold standard a "barbarous relic"—monetary rules fixedly anchored to metal struggle to adjust flexibly with employment and output fluctuations⁵. Bitcoin inherits gold's store-of-value logic and inherits this macro-level fragility: if Bitcoin truly became the primary unit of account and borrowing, its fixed supply would introduce severe deflationary pressure in credit-cycle contractions; the real burden of debt would rise with Bitcoin's appreciation, forming a self-reinforcing deleveraging spiral.

A more immediate problem: Bitcoin's connection to everyday economic activity remains extremely limited. Most goods and services are still priced in fiat; Bitcoin holders face FX conversion when spending; violent price volatility makes it hard to accept as an everyday unit of account. The crux is mainly path dependence: billions of people are already accustomed to fiat pricing; migration coordination costs are extremely high, far beyond what technical feasibility alone can overcome.

Bitcoin's compliance access, however, has taken another path: top-down entry into traditional asset-allocation menus via securitization channels, rather than bottom-up rewriting of retail pricing habits. In January 2024 the U.S. Securities and Exchange Commission approved multiple spot Bitcoin ETFs; as of June 2024, cumulative net inflows into U.S. spot ETFs were on the order of about \$15 billion (Bloomberg/Farside Investors daily aggregates), with BlackRock's IBIT among the main vehicles⁴. Three observable metrics must be distinguished: compliance channels (ETF creations/redemptions, custody disclosure), on-chain settlement flow (true on-chain payments as a share of global payment flow remain marginal—three metrics and data in Chapter 1, Section 8)⁶, and everyday pricing habits (mainstream retail still quotes in fiat). ETF approval changes asset-allocation structure and some volatility patterns—deeper institutional holding may bring more stable allocative buying, or may raise Bitcoin's correlation with traditional risk assets—it does not yet mean Bitcoin has assumed broad unit-of-account or medium-of-exchange functions; a significant gulf remains between institutions "can buy" and the public "can spend."

Section 3. Macroeconomic Implications of Supply Rigidity

To discuss the macro implications of Bitcoin's supply rigidity, three layers must be separated: the gold analogy as store of value, the gold-standard analogy as monetary standard, and the competing-currencies analogy as currency competition. The three are often conflated; their policy implications differ sharply.

In the store-of-value register, supply rigidity is a virtue rather than a defect. Investors buy Bitcoin with logic similar to buying gold or certain scarce assets—hedging long-run erosion of fiat purchasing power, and providing a low-correlation hedge sleeve within a diversified portfolio. This function has no direct effect on overall macro operation, just as private gold holding does not affect monetary-policy effectiveness. Bitcoin's most solid position in the global financial system at present is precisely this layer.

In the monetary-standard register—if the global economy truly shifted to Bitcoin as the standard, all important assets priced in Bitcoin, credit extended in Bitcoin—the macro implications of supply rigidity are entirely different. Any credit expansion would have to rest on Bitcoin lending, and the total cap would mean rates would be truly positive; there would be no “zero-cost liquidity.” Supporters argue this would eliminate moral hazard and force capital toward projects with real returns; opponents note it would periodically trigger severe deflation, leave debt-crisis damage unhedgeable, and remove central banks' buffer of last-resort liquidity in crises. The amplitude of the business cycle might increase substantially.

In the competing-currencies register, Hayek's normative claim must be distinguished from the empirical diversity of on-chain markets. In Chapter 11, “The Possibility of Controlling the Value of a Competitive Currency,” Hayek requires each issuer to “keep the (precisely defined) purchasing power as nearly as possible constant”—competition's pressure direction is toward stable purchasing power, not tolerating a menagerie of inflation targets⁷. On-chain ecosystems present a more mixed spectrum: Bitcoin's fixed supply, Ethereum's adjustable-parameter inflation, fiat-mirrored stablecoins, collateralized public-domain money—these are actual choice outcomes under markets and regulatory fences, and cannot be read backward as Hayek's having advocated “inflation-target competition.” Within sovereign fiat systems, the Woodford–Galí New Keynesian tradition supplies the strongest welfare defense to date for an about-2% inflation target; on-chain, rule suites are left for holders to select—quality is jointly determined by liquidity, verifiable collateral, and switching costs, not by a priori judgment of which rule is welfare-optimal.

On-chain “multiple rules coexist” is an observable fact of market stratification; whether Hayekian “purchasing-power competition” has already occurred at the retail layer must be tested separately against holding structure, switching costs, and peg-maintenance data—one cannot infer that private currency competition has replaced the central bank's objective function merely because multiple tokens are exchangeable in DeFi. Chapter 7's fourth judgment applies equally here: post-depeg repair speed must be checked against collateral state and on-chain verifiability of redemption queues, not judged a priori as “competition already effective” merely because “rules are public.”

Section 4. ERC-20: Interface as Power

In 2015 a developer proposed Ethereum Request for Comments No. 20, the ERC-20 proposal, defining a minimal interface standard of seven functions: `totalSupply` (query total supply), `balanceOf` (query balance), `transfer` (transfer), `transferFrom` (authorized transfer), `approve` (approve), `allowance` (query allowance), plus two events (`Transfer`, `Approval`). Any token contract following this interface can be natively recognized and operated by all wallets, exchanges, and applications on Ethereum without custom integration.

ERC-20's significance far exceeds a technical specification. It created a pool of common knowledge: market participants know how any ERC-20 token operates; infrastructure providers need implement the interface only once to support all compatible tokens; users need not relearn operations for each token. Network effects from such standardization are exponential: Ethereum token counts grew rapidly from hundreds after ERC-20's spread to tens of thousands and hundreds of thousands, forming the largest interoperable token ecosystem to date.

Yet interface standards bring not only benefits but standardized propagation of risk. During the 2016–2017 ICO wave, ERC-20's low threshold let anyone deploy a "token" in hours; whitepaper quality varied widely; many projects were in substance financing fraud packaged as token sales. Satis Group's (2018) independent classification of a 2017 ICO sample judged about 81% scams or high-risk projects⁸—an open interface lowers deployment cost, not identification cost. Markets filtered most speculative projects through liquidity evaporation and price collapse to zero, but losses left to early holders were real. Schumpeter's "creative destruction" displayed itself violently in the ICO frenzy and subsequent market clearing: the cost was high, yet it also accelerated maturation of market capacity to identify token quality—today's professional investors analyzing tokens focus on collateral structure, unlock schedules, governance mechanisms, and real use cases, not mere whitepaper promises.

ERC-20 and its successors (ERC-721 for NFTs, ERC-1155 for semi-fungible tokens, and others) established a principle: within an open-standard framework, a fall in issuance thresholds need not cause a fall in quality thresholds—market competition and auditability can carry the quality-filtering function. For that principle to hold, prerequisites are: market participants can obtain adequate information (on-chain data transparency), and there is no mechanism of forced use of particular tokens (no compulsory licensing). When both hold, accessibility from standardization and market screening can coexist.

Section 5. Transparent Mechanisms of On-Chain Supply Adjustment

Opacity of traditional monetary policy is one deep source of controversy. Even when central banks regularly publish policy-meeting minutes, internal discussion, expected paths of future operations, and weight allocation in actual decisions remain incompletely transparent to market participants. More important, the central bank may buy and sell assets in open markets and affect money supply without prior notice; "monetary-policy transparency" in practice is a limited commitment.

On-chain token supply-adjustment mechanisms in principle offer a fundamentally different transparency. Bitcoin's issuance curve is hard-coded at the protocol layer; anyone can query current circulating supply, mining-reward height, and blocks to the next halving in real time on a block explorer. Parameter adjustments in major DeFi (decentralized finance) protocols—Compound, Aave, MakerDAO, and others—must pass public governance voting; proposal content, voting weights, and results are all on-chain queryable; the specific content and timestamps of parameter changes are permanently auditable in blockchain history.

This auditability has produced real governance dynamics in practice. When MakerDAO lowered DAI stability fees and collateral ratios in 2020, governance discussion underwent weeks of public debate on forums and in on-chain votes⁹; when the 2022 Curve Finance vulnerability triggered emergency parameter updates, the process and reasons were fully recorded on-chain. These events are far from perfect models of democratic governance; governance-token distribution is often concentrated among a few early holders and venture institutions; the substance of "on-chain democracy" sometimes more closely resembles "on-chain oligarchy." Yet compared with traditional monetary policy's opacity, this is at least a transparency that can be studied, criticized, and pushed to improve.

Transparency is not stability. Excessively frequent adjustment of on-chain protocol parameters, and markets' uncertain reactions to governance proposals, can sometimes introduce greater short-term volatility than traditional monetary policy. Extreme stablecoin cases—the UST/Luna 2022 collapse—show that even with fully transparent parameters and fully public rules, design defects can produce transparent collapse rather than transparent stability¹⁰. On-chain transparency is a necessary condition for governance accountability, not a sufficient condition.

Terra/UST's collapse shows that transparent rules do not automatically bring stability. One must ask which mechanism class the failure belongs to: UST mainly relied on LUNA burn/mint and Anchor's high yield to maintain the peg, lacking hard collateral always above 100%—it belongs to **algorithmic stablecoin + undercollateralized expansion**, not MakerDAO/DAI-style CDPs.

Death-spiral chain (Liu et al. 2023; Brunnermeier et al. 2022; CFTC Staff Report 2022; Catalini, Goren & Shah 2021 three-way mechanism taxonomy; He et al. 2023 IMF Fintech Note spectrum preface; Clements 2021 three requirements for algorithmic types; Adams & Ibert 2022 algorithmic-run empirics): UST was algorithmic (third class) rather than overcollateralized CDP (second class); its stability depended on confidence and subsidy sustainability, not hard-collateral coverage at issuance—Clements (2021) noted before the collapse that algorithmic types must simultaneously satisfy baseline demand, arbitrage participation, and reliable price feeds; failure of any one can trigger a run; UST's Curve-pool selling was a joint failure of “oracle + depth”¹¹. Once UST's secondary price broke below \$1, the protocol algorithm minted LUNA to buy UST; LUNA supply surged and price fell; LUNA's fall raised “LUNA quantity that must be burned per unit UST,” absorption capacity weakened, UST depegged further—a self-reinforcing death spiral, different from overcollateralized CDPs' path under shock of “collateral market value shrinks, coverage falls”: the latter has a hard-collateral buffer; the former fills the gap with own-token inflation. Anchor attracted inflows with about 20% UST deposit APY, subsidies paid by ANC inflation; when high yields proved unsustainable, large holders exited first (on-chain data show sophisticated-first exit); liquidity pulled away before retail reaction—tokenomics and stability mechanism failed together. When Terra's collapse contagioned other ecosystems via cross-chain bridges, Board of Governors (2023) ex-post analysis showed that after UST depegged, bridged assets and related DeFi protocols faced synchronized redemption pressure—transparent rules + high TVL can still go to zero within days, and spillovers are not limited to a single chain¹⁰. The SEC's complaint against Terraform Labs (2023) further records from a legal-anatomy angle: UST/LUNA characterized as unregistered securities, Anchor's high yield an unsustainable subsidy—mechanism-class error + regulatory lag can stack; one cannot ignore cross-protocol portfolio risk merely because PCIM is an overcollateralized CDP. Ortiz & Witte (2023) ex-post comparison shows algorithmic stablecoins' redemption speed under stress significantly faster than overcollateralized types (such as DAI)—UST collapsed from nearly \$18 billion circulating within days, while DAI in the same period of ETH crash, though at a premium, maintained redeemability; HKMA RM09-2022 event study distinguishes the two mechanisms' operating stress as “confidence-collapse runs” versus “collateral-shrinkage runs.” Gadzinski et al. (2024) co-instability analysis of a multi-stablecoin panel is consistent: in Terra/LUNA and IRON/TITAN events algorithmic types were the **primary receivers** of shock; fiat-collateralized and crypto-overcollateralized CDPs were relatively more resilient after shock—Congressional Research Service (2022) records from a policy-anatomy angle the path of UST dual-token arbitrage failing after depeg, secondary price once falling to about \$0.12¹⁰. PCIM should be classed with the latter, and must use C_0 , x^* and reserves R to lengthen run time—one must not infer from UST's transparent collapse that “all on-chain stability rules share the same fate.”

PCIM/VRC-10 deliberately demarcates from UST on the spectrum—current tier $C_0 > 100\%$ overcollateralization (upper tier about 161.8%), prohibition of filling gaps by dual-token burns alone, prohibition

of high own-token yield subsidies on the stablecoin. Competitive issuance changes issuer count and rule transparency, not the VRC-10 public-domain layer's hard constraint that "on-chain hard collateral must cover face debt" ($C_0 > 100\%$)—VRC-11's private-domain layer is 61.8% low collateralization, with structural gap $g(0) = 38.2\%$ counted separately. If Bitgold and the BTG ecosystem crash together, overcollateralization likewise faces redemption runs and falling coverage; UST's lesson is a warning of class error, not proof that "no liquidation line" immunizes against black swans. VRC-11's private-domain layer uses 61.8% low collateralization—another risk class, not to be conflated with VRC-10 overcollateralization. Momtazi's (2022) ex-post survey attributes Terra's collapse to the triple stack of algorithmic mechanism, Anchor subsidies, and governance concentration¹²—item-by-item against the pit list PCIM must avoid; Lyons & Viswanath-Natraj (2020) show that even fiat-collateralized USDC's peg still depends on reserve redeemability and OTC depth, not reserve statements alone¹². Open questions remain: cross-protocol portfolios may still introduce undercollateralized stable assets indirectly into the PCIM ecosystem as "reserves"—red-line compliance at the single-protocol level is not system immunity.

Section 6. Spontaneous Division of Labor Between Bitcoin and the Token Ecosystem

The on-chain monetary ecosystem that evolved in reality is not the result of anyone's prior plan, but of market selection performing layered adaptation under multiple constraints. Bitcoin, Ethereum, various stablecoins, and VRC protocols occupy different functional positions in this ecosystem, competing and complementing one another.

Bitcoin in this ecosystem increasingly firmly carries the dominant store-of-value narrative. Its community explicitly opposes any modification that would destroy fixed-supply properties; Bitcoin ecosystem development focus is on extending security and enhancing Bitcoin's usability in the broader financial system (Lightning Network for small payments, Bitcoin ETFs for institutional access), not on extending its smart-contract functionality. That character makes Bitcoin the crypto asset with the highest degree of institutional adoption, but also leaves it relatively limited in decentralized-finance applications.

Ethereum and its compatible chains carry the vast majority of smart-contract applications, stablecoins, DeFi protocols, and NFTs. The ERC-20 standard established Ethereum as the core platform of the composable token ecosystem. Yet Ethereum's historical evolution—from proof of work to proof of stake ("The Merge," 2022), from high-gas single-chain architecture to Layer-2 rollup scaling—shows it is a technical and governance system in continuous change, lacking Bitcoin's near-sacralized rule immutability. Ethereum's flexibility is the source of its application value and also the reason its "monetary properties" are relatively constrained.

Fiat stablecoins (USDT, USDC, and others) play the de facto primary value-transfer medium role in everyday trading, DeFi yields, and cross-border remittances. They trade price stability for centralized custody (reserves of equivalent dollar assets). A prior limit: Hayek's Chapter 11 test standard is an autonomous unit of account with purchasing power kept as constant as possible, not an extension tool mirroring fiat—by that standard, USDT/USDC remain fiat extensions rather than autonomous monetary systems; if one relaxes to "widely circulating privately issued value tools," then the most popular on-chain stability tools are precisely those most dependent on the existing fiat system. Keynes's systematic account of "liquidity preference" in the *General Theory*—in uncertain times people tend to hoard monetary assets that can be realized immediately rather than bear risk—helps explain stablecoins' excess demand in volatile markets¹³. This reality shows that the crypto ecosystem's present stage of development still largely takes fiat value as its reference coordinate.

Stablecoins' sudden rise approaches, in a sense, the first step Hayek envisioned of "private money gaining wide use": privately issued value tools have gained large-scale circulation on global chains. Tether (USDT) on-

chain circulating market cap once exceeded \$120 billion in 2024 (CoinGecko and Tether Transparency monthly disclosures¹⁴); USDC over the same period was on the order of about \$34 billion¹⁴—scale already comparable to M2 subcomponents of several mid-sized economies, yet whether and how they pass through domestic monetary-policy transmission still lacks cross-country panel-level causal identification. Chainalysis’ *2024 Geography Report* shows Argentina, Turkey, and other high-inflation economies with stablecoin on-chain receive intensity significantly above the global mean⁶—this is an observable association, not sufficient evidence that “monopoly is already broken.” Yet stablecoins have not truly realized the autonomous monetary system Hayek hoped for—they are digital mirrors of the dollar; their stability depends on dollar credit; their operations depend on tacit acceptance within U.S. regulatory frameworks. USDC issuer Circle maintains close compliance relations with U.S. regulators; USDT’ s reserve composition and compliance status have long been contested. These two cases show that under the existing international monetary system, if private stablecoins are to gain sufficient scale and trust, they almost inevitably must hook to the dollar system and its regulatory framework—which precisely limits their possibility as an independent monetary order.

Openverse’ s VRC protocol family attempts to build a more complete monetary-system hierarchy: VRC-10 (Bitcurrency, public-domain money standard) issued with Bitgold overcollateralization; VRC-11 (Privcurrency, private-domain stablecoin) issued at 61.8% low collateralization within permissioned domains; VRC-12 (Bitsecurity, equity-type tokens) connecting RWA; VRC-13 providing standards for time-type assets. The design ambition is, through protocol-internal anchoring on the Layer 0 value-exchange layer (Bitgold as reserve base), to build a composable multi-currency structure on the Layer 1 application layer, while lowering public-domain money’ s issuance threshold through PCIM (Public Currency Issuance Mechanism)—nominally mapping to various sovereign fiat units, with supply constrained at the base by dynamic-tier collateral ratios (upper tier about $C_0 \approx 161.8\%$), rather than simply anchoring central-bank liabilities.

The Openverse whitepaper (v2.1.5) casts itself as an experiment that completes payment and stable unit-of-account capacity on Bitcoin’ s legacy (official copy calls it “Bitcoin 3.0”; this book cites it only as the design’ s self-description): Bitcoin’ s achievements in censorship-resistant store of value are outstanding, yet energy use, throughput, confirmation latency, price volatility, and on-chain fees make it hard to bear mass payments—Poon & Dryja’ s (2016) Lightning Network whitepaper tries to ease small-payment friction with off-chain channels, but the settlement layer remains anchored to BTC volatility¹⁵; USDT and other centralized stablecoins fill the “constant value” gap yet reconcentrate credit on corporate balance sheets. Public-domain money tries to realize on-chain simultaneously verifiable collateral, parallel multi-fiat units, and open participation—inheriting Nick Szabo’ s “bit gold” (2005: verifiable proof of work creates unforgeable scarce bits, distributed property registration) and Hayek’ s intellectual resources on competing currencies, with a Layer 0 global decentralized value-exchange layer (PoS consensus, final-settlement anchoring, VTP cross-chain routing) as base, so that in-ecosystem application chains and external Layer 1 networks can all connect, rather than a closed Hub/Zone LAN¹⁵. The whitepaper also admits frankly: the ambition of public-domain money to “partly replace fiat” far exceeds what most jurisdictions currently tolerate, belonging to the same class of institutional friction Libra once met—a gulf between thought experiment and political reality that technology alone cannot fill.

Section 7. Competition Among Cross-Chain Standards: Protocol Interoperability and Value Lock-In

As on-chain asset scale grows, multi-chain ecosystem interoperability problems become increasingly salient. Holders cannot use tokens on chain A directly in applications on chain B, giving rise to cross-chain bridges as an infrastructure category. Yet the history of cross-chain bridges is almost a history of security incidents: in 2021–

2022, Ronin (about \$625 million), Wormhole (about \$325 million), Nomad (about \$190 million), and others were successively attacked; Chainalysis (2022) tallied about \$2 billion stolen in cross-chain bridge hacks that year¹⁶. Such losses reflect structural fragility in bridge design itself: bridge protocols must maintain a set of contracts and verification mechanisms on each of two chains; a vulnerability on either side can empty the bridge’s assets—Board of Governors (2023) analysis of cross-chain contagion after Terra’s depeg also shows that the bridge layer can amplify systemic risk.

This fragility prompted rethinking of cross-chain interoperability standards. IBC (Inter-Blockchain Communication) is the cross-chain communication standard developed in the Cosmos ecosystem; its design philosophy is: create no intermediate custody layer; let the two chains directly verify each other’s consensus proofs, securing cross-chain transfers with cryptography rather than intermediaries. The IBC model has clear security advantages but requires both chains to support the IBC standard; integration with large public chains such as Ethereum still faces technical challenges.

VTP (Value Transfer Protocol) is Openverse’s proposed cross-chain value-transfer standard—positioned analogously to HTTP for the internet: providing a standardized cross-chain value-transfer interface so that assets on different chains can complete transfer and settlement in standardized ways without developing bridge logic for each pair of chains. Only if VTP passes stress tests and achieves design goals might it push the on-chain monetary ecosystem toward “internetization”—just as HTTP unified data transmission among different network nodes, VTP’s goal is to unify value transmission among different value ledgers; until then, IBC and other production standards and various custodial bridges will long coexist.

Competition among cross-chain standards is in substance a power contest over “who defines the foundational rules of on-chain value transmission.” It deeply resembles early internet protocol standards wars: TCP/IP’s victory owed less to maximal technical elegance than to sufficient simplicity and openness, and adoption by critical nodes. On-chain standards’ adoption logic is similar—technical superiority is necessary but not sufficient; quality of developer tools, strength of ecosystem support, and adoption rates of critical applications matter equally.

Section 8. The First Meaning of Popularization: Issuance Thresholds Fall Sharply

At this point, the first meaning of “monetary popularization” can be summarized: issuance qualification shifts from licenses to code, from institutions to protocols, from political authorization to publicly deployable standards.

In traditional monetary systems, money issuance is among the most strictly regulated privileges. Issuing fiat requires state sovereignty; issuing bank deposit money requires a banking license, satisfying capital adequacy, reserve requirements, and strict supervisory review; issuing money-like instruments (checks, bills of exchange, payment tokens) requires corresponding payment-service licenses. These thresholds have institutional logic—preventing over-issue, protecting holders, maintaining system stability—but they are also powerful barriers to market entry, in practice confining money issuance to a few licensed institutions.

ERC-20 lowered the threshold for “issuing interoperable tokens” to: a computer, tens of dollars of fees on Ethereum, and publicly available contract templates. The EIP-20 specification hardens interface semantics for `transfer/approve/balanceOf` and related functions; Wood’s Yellow Paper §4.2 casts token transfers as state-machine transitions; Buterin’s (2014–2015) *Design Rationale* clarifies account-model and gas-metering trade-offs—individuals, organizations, or protocols need no license, capital review, or regulatory approval to deploy a fully functional token contract within hours¹⁷²—money issuance shifts from privilege to open engineering choice.

Protocolization of thresholds releases part of the issuance impulse formerly locked inside institutional licenses; consequences are mixed and must be screened by markets after the fact, not by prior approval.

This openness brings not only efficiency but chaos that needs new filtering mechanisms: among hundreds of thousands of tokens, the vast majority are destined to go to zero. Filtering relies mainly on markets' ex-post screening—liquidity depth, holder dispersion, protocol audit reports, real application scenes, developer-ecosystem activity—rather than regulators' ex-ante approval. These indicators jointly constitute a new threshold of “on-chain market access,” with logic entirely different from traditional regulatory licenses: it is open but costly, observable but also manipulable, decentralized but also productive of new information asymmetries.

PCIM (Public Currency Issuance Mechanism) pushes this logic to the public-domain money layer: through a standardized Bitgold collateral process, any participant meeting collateral conditions can participate in Bitcurrency issuance, opening to a broader set of market participants the money-creating capacity that once belonged only to banking—namely “on the basis of collateral assets, issue circulating money.” What is opened is participation qualification and rule visibility, not abolition of collateral constraints; money creation must still obey on-chain verifiable staking and redemption conditions.

Compared with traditional banks' credit creation, the core difference PCIM claims at the documentation layer lies in information symmetry and rule predictability. Traditional banks expand monetary credit to borrowers through internal credit approval on a deposit base; the process is almost opaque to external observers—asset quality, reserve status, credit concentration all sit in banks' internal systems; outsiders can glimpse only through quarterly reports and regulatory disclosure. PCIM' s collateralized issuance process, when deployed as designed, is recorded end-to-end by on-chain contracts: collateral type and value, issuance amounts, real-time changes in collateral ratios—any node can verify. Issuance rules do not vary by issuer identity; all participants operate under the same protocol constraints. Whether this transparency suffices to support public trust and to compete with traditional banking on macro stability still requires testing after scaled operation, and cannot be extrapolated from a whitepaper alone as a completed institutional experiment.

The first meaning of popularization—the fall in issuance thresholds—is the most perceptible dimension of on-chain monetary change, and the one that most directly touches traditional monetary institutions, but it is only the first layer. Whether holding rules can be publicly audited, whether governance rights can be substantively exercised, whether the monetary system can be imagined as public infrastructure—all build on this layer. The standards contest Bitcoin opened is fundamentally about who sets monetary thresholds and to whom they open; after standards land, incentive structure determines whether participants stay.

The fall in issuance thresholds itself also does not equal a rise in monetary quality. In traditional systems, licensing, though monopolistic, also bound some degree of compliance requirements and financial-soundness review into issuance rights. The opened on-chain environment removes that binding: anyone can issue, anyone can hold; market filtering replaces regulatory screening. This mode is more efficient, but the reality of harm is also higher—countless ordinary users have paid real losses before immature market mechanisms. The challenge for PCIM and the VRC protocol system is how, while keeping open participation, to build sufficiently robust protocol-native constraints so that falling thresholds truly evolve into improved accessibility of quality money, not merely a flood of junk assets.

注释与引用

1. BIS et al. (2020), *Foundational Principles and Core Features*, Principles 1–3 (CBDC as cash extension, coexistence with existing systems); Niepelt (2024), *CBDC: Whence, Why, What, and How*, MIT Press, chs. 1–2: the state path upgrades the ledger with a public monetary anchor; the protocol path supplies parallel discipline with verifiable collateral—see Chapters 8–11. ↩
2. Easley, David, Maureen O’ Hara, and Soumya Basu. “From mining to markets: The evolution of bitcoin transaction fees.” *Journal of Financial Economics* 169, 2025, pp. 103892 (fee-market evolution after declining block rewards); Buterin, Vitalik, “Ethereum Design Rationale,” 2014–2015 (account model, Gas, state-tree trade-offs; cross with Wood Yellow Paper §§1–4). <https://doi.org/10.1016/j.jfineco.2024.103892> ; <https://github.com/ethereum/wiki/wiki/Design-Rationale> ↩ ↩²
3. Chapter 3, Section 2 ⁷; Chapter 1, Section 6 ¹⁰: three QE rounds about \$3.7 trillion, distribution, and “correlation ≠ causation”; Bernanke (2015), *The Courage to Act*, chs. 7–9. ↩
4. SEC (2024-01-10) approval of multiple spot Bitcoin ETFs; Farside Investors daily net-inflow aggregates (June 2024 cumulative about \$15 billion order of magnitude): <https://farside.co.uk/btc/> ; Tesla 10-K/10-Q (2021–2022): February 2021 disclosure of about \$1.5 billion purchase; 2022 sale of about 75% of holdings. ↩ ↩²
5. Keynes (1923), *A Tract on Monetary Reform*, ch. 4: “In truth, the gold standard is already a barbarous relic, and it is hard to believe that it will long survive the war.” Project Gutenberg: <https://www.gutenberg.org/ebooks/32637> ↩
6. McKinsey Global Institute (2024), “The Future of Payments”: on-chain payments about 0.02% order of magnitude of global payment flow; Artemis Analytics on-chain payment statistics cross-reference; Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*: stablecoin receive intensity in Argentina, Turkey, and other high-inflation economies. <https://www.chainalysis.com/geography-of-crypto/> ↩ ↩²
7. Hayek (1976), *Denationalization of Money*, pp. 46–47 (ch. 11): issuers must “keep their (precisely defined) purchasing power as nearly as possible constant”—competition approaches stable purchasing power, not diversity of inflation targets. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf>; Woodford (2003), *Interest and Prices*, chs. 6–7; Galí (2015), chs. 8, 15. Sovereign NK defense and boundaries of on-chain rule competition: Chapter 10, Section 8; Chapter 24, Section 2. ↩ ↩²
8. Satis Group (2018), “Cryptoasset Market Coverage Initiation: Network Creation”: about 81% of 2017 ICO sample classified as Identified Scams or Failed/Dead Projects (independent classification; see original for definitions). ↩
9. Schär (2021), *Federal Reserve Bank of St. Louis Review* 103(2), pp. 153–174: MakerDAO/DAI CDP and on-chain governance overview; MakerDAO Risk Team (2020-03-12), “Black Thursday Post Mortem”: liquidation spiral and subsequent parameter increases. Forum: <https://forum.makerdao.com/t/black-thursday-post-mortem/1853> ↩
10. Liu, Makarov & Schoar (2023), NBER WP 31160 “Anatomy of a Run: The Terra Luna Crash”: on-chain data show Anchor high-yield subsidies unsustainable, large holders exiting first; Brunnermeier, Niehaus & Schab (2022), BIS Bulletin No. 63; Catalini, Goren & Shah (2021), MIT Sloan RP: three-way taxonomy of stability mechanisms (fiat-collateralized / crypto-overcollateralized / algorithmic) and conditions for unsustainable subsidies; He, Dong, Ross Leckow, Tommaso Mancini-Griffoli, and Hiroshi Nagaoka (2023), IMF Fintech Notes 2023/001: stablecoin mechanism spectrum and run risk; IMF (2022), *GFSR* October issue ch. 2 pp. 43–78; HKMA RM09-2022: May 2022 stablecoin depeg event study; CFTC Staff Report (2022): Terra/Luna death-spiral mechanism; Board of Governors (2023), FEDS 2023-044: cross-chain bridge and related DeFi contagion spillovers after Terra depeg; Ortiz & Witte (2023), BIS WP 1137: algorithmic vs overcollateralized run-speed contrast; Gadzinski, Castello, Liuzzi & Sargenti (2024), *International Review of Financial Analysis* 96, 103608: Terra/LUNA co-instability and CDP resilience contrast; Congressional Research Service (2022), IN11928: UST/LUNA dual-token arbitrage and policy anatomy of depeg to about \$0.12; SEC v. Terraform Labs complaint (2023-02-16). ↩ ↩² ↩³ ↩⁴
11. Clements, Ryan (2021), “Built to Fail: The Inherent Fragility of Algorithmic Stablecoins,” *Wake Forest Law Review Online* 11, 131–171 (three requirements for algorithmic types); Adams, Austin, and Markus Ibert (2022), “Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel,” *FEDS Notes*, June 2, 2022; Auer, Raphael, et al. (2023), “The Technology of Decentralized Finance (DeFi),” BIS Working Paper 1066, §4 Terra/UST Curve-pool run. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3952045 ; <https://doi.org/10.17016/2380-7172.3121> ; <https://www.bis.org/publ/work1066.htm> ↩

12. Momtazi (2022), *Journal of Risk and Financial Management* 15(11), 520: Terra algorithmic mechanism, Anchor subsidies, and governance concentration triple failure; Cong, Li & Wang (2024), *Journal of Financial Economics* 151, 103745: Anchor-style subsidy dynamic adoption; Lyons & Viswanath-Natraj (2020), NBER WP 27136: reserve redeemability and peg; Ferraro, Kan & Sunderam (2022), Princeton Economics WP 1416 “Stable Coins but Thin Markets”: OTC thin-market peg fragility. <https://doi.org/10.3390/jrfm15110520> ; <https://www.nber.org/papers/w27136> ↩ ↩²
13. Keynes (1936), *The General Theory of Employment, Interest and Money*, ch. 13: sets out liquidity preference—people’ s preference for holding money rather than other assets, arising from uncertainty about future rates and asset prices. Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩
14. CoinGecko API historical market-cap series (USDT/USDC, 2024 peak range); Tether Transparency monthly reserve disclosures: <https://tether.to/en/transparency/> ; Circle USDC reserve reports: <https://www.circle.com/en/usdc> ↩ ↩²
15. Szabo (2005), “Bit gold”: verifiable PoW creates scarce bits, minimizing trusted third parties; Nakamoto (2008), §§1–2 (P2P electronic cash and timestamp server); Poon & Dryja (2016), *The Bitcoin Lightning Network* (off-chain micropayments); Openverse Foundation, *Bitgold Whitepaper* v2.1.5 (source: official whitepaper v2.1.5, not independently audited). <https://unenumerated.blogspot.com/2005/12/bit-gold.html> ; <https://bitcoin.org/bitcoin.pdf> ; <https://lightning.network/lightning-network-paper.pdf> ↩ ↩²
16. Chainalysis (2022), “2022 Crypto Crime Report”: cross-chain bridge hacks 2022 cumulative about \$2 billion; Ronin (2022-03, about \$625 million), Wormhole (2022-02, about \$325 million), Nomad (2022-08, about \$190 million) line items in respective protocol post-mortems. ↩
17. EIP-20 (2015), ERC-20 Token Standard: transfer/approve/balanceOf interface semantics; Wood, Gavin, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Yellow Paper, §4.2 (Gas and state transition); Buterin (2014), *Ethereum White Paper*, §“Decentralized Applications” (source: official whitepaper, not independently audited). <https://eips.ethereum.org/EIPS/eip-20> ; <https://ethereum.github.io/yellowpaper/paper.pdf> ; <https://ethereum.org/en/whitepaper/> ↩

§ 13 Incentive Structures in Tokenomics

Standard interfaces lower issuance thresholds and interoperability costs, but standards alone do not guarantee continued use. Once the threshold falls, one must ask: who receives tokens under what conditions, how tokens return to the protocol, and whether inflation or deflation serves the network's long-term health. Tokenomics looks like parameter setting on the surface; in substance it is an institutional experiment in incentives, constraints, and long-run sustainability—whether on-chain incentives can substitute for parts of traditional reputation mechanisms, how cold starts and over-incentives set traps, and what political economy governance tokens bring, all of which must be tested against cases of success and failure.

Section 1. Incentive Visibility: On-Chain Rules Replacing Black-Box Arrangements

In September 2022 Ethereum's "Merge" switched consensus from proof of work to proof of stake, cutting annual inflation from roughly 4% to about 0.5%¹—a contemporary sample of a hard switch in incentive structure completed through on-chain governance and client upgrades. Parameters written in code do not mean society has broadly accepted the new rules: node forks and client-compatibility disputes before and after the Merge show that technical feasibility and institutional adoption must be tested separately—as Chapter 6 argued, active on-chain settlement is not the same as retail pricing habits having migrated.

Traditional finance runs on a set of constraints that are not always transparent. Banks maintain capital adequacy; regulators inspect periodically; reputational capital forms an intangible constraint—yet the internal logic of that system is often closed to ordinary depositors. How a bank allocates lending profits, sets internal risk thresholds, or how bonus structures shape risk appetite—such information hides behind the jargon of compliance reports; the public can scarcely judge.

On-chain protocols write many constraints as publicly readable contract code: token release schedules, staking requirements, liquidation thresholds, treasury allocation ratios. The public can read the rules before participating and audit execution afterward. Transparency comes from the architecture's forced openness—blockchain data and deployed contract code are, in principle, readable by anyone—not from the issuer's voluntary promises in marketing materials.

The 2020 liquidity-mining wave displayed this incentive visibility most vividly. Compound distributed COMP governance tokens to both depositors and borrowers as rewards for protocol use, driving DeFi total value locked (TVL) sharply higher within the incentive cycle—ecosystem-wide TVL rose from roughly the \$1 billion order of magnitude in early 2020 to a peak above \$180 billion in November 2021, then fell below about \$50 billion after incentives receded in 2022². Who was farming, at what scale, and when they exited—every operation is recorded on Ethereum block explorers. That contrasts sharply with the secret preferential rates traditional institutions grant large clients.

Visibility does not eliminate information asymmetry; it changes its structure. Nested contracts remain hard for ordinary users to parse—a DeFi protocol with multi-layer calls may produce security-audit reports dozens of pages long that users cannot independently read. The key change is that audit is possible. Professional security firms, academic researchers, and technical community members can unpack contract logic and disseminate conclusions in readable form. The role of information intermediaries shifts from "whether to grant access" to "how to help understand information already public."

That change matters substantively for Tokenomics discussion: white-paper descriptions detached from concrete on-chain addresses and real data have limited reference value. Promises on paper rather than in code depend for their force on the project's integrity, not on the protocol's technical structure. Assessing a tokenomic design must start from on-chain data—whether allocation matches the white paper, whether the treasury is used as specified, whether large holdings show signs of manipulation. That is the background against which on-chain audit culture has gradually formed.

Section 2. Cold Start: How New Protocols Ignite Initial Liquidity

Every new protocol faces a cold-start dilemma: without users the protocol has no value, yet without value users will not come. This is a classic coordination game, not unique to blockchain—banks need depositors and borrowers simultaneously; markets need buyers and sellers. Traditional solutions usually build physical infrastructure, brand endorsement, or rely on regulatory licenses that compel participation. On-chain protocols address the problem with token incentives: extra tokens to early participants front-load the cost of starting the protocol along the time axis, exchanging future value for present liquidity.

The mechanism is popularly called “liquidity mining” or “farming.” Short-run data often look brilliant—high annual percentage yields (APY) attract capital quickly; TVL curves rise steeply. The core question behind the numbers is: what endogenous utility does the token have beyond the incentive itself? In *The General Theory*, Keynes described “animal spirits” driving investment as spontaneous urges to action beyond pure rational calculation—protocol cold starts likewise depend on such confidence: early participants must believe future network value will cover present risk³.

Endogenous utility can be pursued in four directions: governance rights (holders vote on protocol parameters; if the protocol has value, governance has value); fee sharing (fees distributed proportionally to stakers); staking security (tokens as a safety buffer; stakers bear liquidation risk for yield); ecosystem grants (treasury funding ecosystem building). If any one of these utilities can hold over the long run, incentive distribution has a sustainable logic; if none holds, the structure slides toward “infinite issuance to reward earlier participants paid by later capital”—a Ponzi structure.

Successful cold starts often share a pattern: high initial rewards attract first liquidity; after network effects form, subsidy ratios gradually fall; meanwhile real use cases—trading fees, lending spreads, cross-chain settlement demand—are continually optimized so that protocol revenue becomes the real support for token value. Uniswap's fee-distribution debates, Aave's safety-module design, and Curve's veCRV lock mechanism all try, in different dimensions, to answer how holding becomes a real value proposition rather than pure speculation.

Failed cases are relatively easy to identify: supply curves tied only to marketing milestones, not to growth in use. When reward growth persistently outruns real protocol use, the token-incentive cost per unit of use keeps rising—economically unsustainable. Early exiters gain; late participants bear liquidation risk—the death spiral of over-incentive—which in bear markets often ends in price cascades and protocol abandonment.

When assessing on-chain projects, cold-start subsidies must be distinguished from over-incentive: the key is not “whether tokens are issued,” but whether the rate of incentive release can keep pace with real value growth. When TVL curves are steep while real protocol revenue (fees, spreads, settlement volume) lags, high APY more likely reflects subsidy than adoption—TVL must not be misread as “competing money already socially accepted.”

Section 3. Token Release: Inflation Curves and Value Anchoring

If cold start answers “how to ignite,” the release curve answers “how to sustain.” Almost every protocol that issues a fixed-supply token faces a release schedule: when team allocations unlock, when investor allocations

become liquid, how community incentive pools release year by year. That schedule directly determines market supply and thus price and holder behavior.

Accelerated release of a fixed total is a common mistake. Early floods of tokens into the market, if demand grows slower than supply, pressure prices; price pressure undermines holding confidence and adds selling pressure—a negative feedback loop. Messari’s 2022 token-unlock tracking showed that many projects issued in 2021 drew down more than 90% from peak in the subsequent bear market⁴—an observable consequence of mismatch between release curves and real demand, not the accidental failure of isolated projects.

Healthier designs usually share several features: team and early-investor allocations with sufficiently long lock and vesting periods to align long-term interests; community incentive shares released dynamically against actual protocol use rather than by calendar; burn or lock mechanisms that lower circulating supply so protocol growth can reflect in token price and build positive feedback.

Bitcoin’s fixed 21-million supply and four-year halving cycle remain the most widely referenced case in on-chain tokenomic design. Halving’s essence is designing the release curve as a known disinflationary path, giving early holders strong reason to hold long while keeping miner (protocol security provider) incentives economically attractive under rising-price expectations. The design is imperfect—its strict fixity cannot respond dynamically to developmental stages—but it set an extremely high bar for predictability and credibility.

The Openverse white paper (v2.1.5) positions Bitgold (BTG) with two distinct functions that must stay consistent with public-currency terminology. **Monetary-economic function:** as collateral reserve for PCIM and VRC-10/11/12, constraining issuance capacity for public currency, private-domain stablecoins, and security-type tokens—it does not serve as a daily payment medium; the VRC-10 public layer must issue under dynamic-tier overcollateralization (upper tier $C_0 \approx 161.8\%$), the VRC-11 private-domain layer at 61.8% undercollateralization, and VRC-12 with independent staking parameters—the three must not be conflated. **Network-operation function:** staking asset for POS consensus and medium for on-chain fees—infrastructure-layer roles of any PoS native token, not a second “monetary use.” The white paper sets total supply at 200 million with a three-year halving, drawing analogy to the order of magnitude of historical gold extraction; when the issuance curve lands as designed, it will constrain Bitcurrency’s collateralized issuance ceiling and link to VRC-12 staking parameters—whether release rhythm matches collateral demand still requires operating data. Bitgold’s Tokenomics embeds, under this framework, the value-foundation layer of the whole protocol suite; if release rhythm keeps selling pressure above demand growth, or collateral prices plunge in a bear market, the stake-issue-redeem chain will bear cascading pressure—comparable statics with overcollateralized CDPs under shock.

Section 4. Governance Tokens and the Political Economy of On-Chain Democracy

Governance tokens bind “money” and “voting rights,” creating a hybrid rights structure without a counterpart in traditional finance. Holders may vote on fee adjustments, treasury spending, upgrade paths, whitelisted assets, risk parameters, and more. Functionally it resembles a hybrid of “shareholder—central bank”: claims on surplus allocation (shareholder-like) and votes on monetary policy and liquidity management (central-bank-committee-like).

The appeal is direct stakeholder participation. Real users, long-term holders, and development contributors can, in theory, express preferences on protocol direction through votes, breaking the “silent minority shareholder” dilemma of traditional corporate governance. In an early crypto industry dominated by centralized exchanges, this was a real innovation in power structure.

In practice, governance systems face stubborn problems. First, whale capture: one-token-one-vote gives large holdings overwhelming influence over proposals; in thin governance-token markets, “governance attacks”—buying enough voting power cheaply to steer proposals—are theoretically feasible and already recorded. Second, low turnout: many holders ignore proposals, so a few active participants dominate, not necessarily representing long-term holder interests. Third, short-termism: the ability to buy tokens quickly, vote, and sell tilts some decisions toward short-run price interests rather than long-run protocol health.

The industry has tried many remedies. Timelocks delay execution after passage to give the community reaction time; delegation lets ordinary holders entrust votes to professional governors; quadratic voting lowers large-holder influence via square-root counting; veToken mechanisms (such as Curve’s veCRV) require long locks for full voting power, binding governors’ time interests to the protocol’s long run.

One-token-one-vote under concentrated holdings can effectively degenerate into oligarchic banking—Beanstalk’s 2022 flash-loan attack showed that borrowing votes, voting, and withdrawing within a single block can breach defenses before a timelock takes effect⁵. Aquilina et al. (2023) BIS post-mortem analysis further shows that stablecoin and DeFi governance-token issuance and voting power are highly concentrated, with run contagion and governance capture structurally aligned—a few addresses can simultaneously affect peg parameters and liquidity-exit order⁶. A debatable protocol-side response is to rule-ify “changing the rules” itself: collateral parameter C_0 and the competitive-issuance switch require independent quorum and maximum-delay timelocks; flash-loan governance must be banned at the contract layer or require a voting-power warm-up (votes count only after holding for T blocks); emergency pause opens only additional collateral and redemption, forbidding unilateral balance-sheet expansion. If in crisis a proposal would cut C_0 or expand unilaterally, it must meet split-track quorum and maximum timelock so markets and smaller holders can exit or add collateral beforehand—Maker and Terra governance histories both contain parameter contests. During UST’s May 2022 depeg, Terra used governance proposals to deploy BTC reserves for a “bailout”; even with transparent voting procedure, mechanism-category error (algorithmic undercollateralization + high-yield subsidy) made governance delay collapse rather than reverse the death spiral—unlike Beanstalk-style “flash capture,” a lesson in slow capture + wrong Tokenomics. Open questions remain: under high concentration, constraints may still be eroded by staged passage or long lobbying; on-chain systems cannot replace courts in holding malicious governance accountable; crisis governance still reacts slower than central-bank midnight coordination—this book narrows the governance discussion to “capture risk is observable,” not “power is already dispersed.” Maker later introduced external liquidity modules such as D3M through governance; the 2023 Endgame plan further split the protocol into SubDAOs and restructured the MKR governance token—showing that PCIM must accept fixed C_0 used jointly with ex-post revision; parameter changes must be monitorable ex ante and accountable ex post, not idealized as “never change parameters”⁵.

Governance tokens also face regulatory-classification uncertainty. They are neither traditional equity (no legal shareholding), nor pure public-goods tokens (they exert real control over parameters), nor money (not legal tender). Major jurisdictions still diverge sharply on whether governance tokens are securities. Protocol designers must preset compliance interfaces early—KYC requirements, geographic limits, securities exemptions—rather than assume perpetual residence in a regulatory gray zone.

Section 5. Burn Mechanisms: Turning Use into Value Recirculation

Token burns have become a widely adopted supply-management tool. Protocols use part of trading fees to buy tokens on the market and permanently destroy them, directly reducing circulating supply. In theory, more use means more burn and greater holder benefit—positive feedback akin to share buybacks. Ethereum’s EIP-1559,

which automatically burns base gas fees, is the most representative implementation: after the 2022 Merge, high-activity months saw net negative issuance; Ultrasound.money on-chain statistics allow day-by-day checks of burn versus issuance⁷—observability is not proof of long-run equilibrium; gas demand fluctuates with cycles, and burn intensity alone cannot sustain a “deflationary money” narrative.

The key to burn design is trigger conditions and scale. If burn funds come from protocol revenue (fees), the mechanism naturally converts use growth into holder value—logically coherent. If burn funds come from newly issued tokens (“print new goods to buy old goods to burn”), the deflation is cosmetic; substantively it is inflation relocated, creating no real value.

When analyzing a token’s long-run value proposition, burns must be read with the issuance curve: net supply = new issuance - burn. If net supply stays positive and faster than adoption growth, holding pressure persists; if net supply tends toward balance or turns negative as the protocol matures, holding has real economic reason. Such judgments belong in continuous on-chain tracking, not white-paper rhetoric.

If Openverse blue papers bring Bitcurrency’s circulating layer into automatic burn hedged against PCIM collateralized issuance, that could in theory raise supply elasticity—whether VRC-10 and VRC-12 incorporate burn or buyback still requires operating data and independent audit; long-run health must not be inferred directly from white-paper roadmaps.

Section 6. Comparison with Fiat Incentive Systems

Placing on-chain Tokenomics beside fiat monetary systems aims to identify each system’s accountability interfaces and failure modes—not to declare which is superior.

Fiat systems constrain monetary policy through multiple institutional layers: independent central-bank charters, congressional mandate targets (such as dual employment–inflation goals), macroprudential frameworks of financial-stability committees, and lender-of-last-resort mechanisms. Accountability includes congressional hearings, media coverage, academic research, and electoral pressure. In *The General Theory*, Keynes assigned central banks the crisis role of “lender of last resort,” supporting the financial system with liquidity—an important source of postwar macroeconomic-stabilizer thought⁸. These mechanisms are imperfect—political cycles affect independence; crisis bailouts are contested—but they are multilayered, historically tested accumulations of institutional design.

On-chain protocols constrain policy through code and governance: parameters in contracts, upgrades via on-chain proposals, critical operations under timelock. Accountability interfaces are on-chain proposals and votes, public audit reports, and repository change logs. Failure modes include contract bugs (hacks), governance capture (whale control), and oracle manipulation (bad prices causing wrong liquidations)—mechanism analysis of governance capture and debatable protocol responses appear in Section 4.

In Chapter 12 of *The Denationalization of Money*, Hayek summarized the selection mechanism: under abolition of forced legal tender and market-adjustable relative prices, holders vote with their feet; money flows to units of most stable purchasing power and most verifiable information—“good money can come only from self-interest, not from benevolence” appears here as profitable dumping of the inferior and retention of the superior⁹. On-chain reality is messier: high-APY liquidity mining, meme narratives, and dollar-mirror stablecoins coexist, showing that rule verifiability is partly achieved while social-level monetary choice is still distorted by information costs, liquidity depth, and regulatory fences. Paper-era clearinghouse discount reflux is often replaced on-chain by high-APY subsidies and meme narratives: surface liquidity can be ample while delaying rather than accelerating Thiersian quality screening—settlement volume, redemption depth, and OTC/DEX deviation must all

enter observable metrics¹⁰. Tokenomics is therefore not only a parameter game but encoding choice signals into observable state: collateral coverage, mint/redeem same-price, supply curves, and governance timelocks should be the public's verifiable basis for "choosing money," not white-paper promises alone—whether stability constraints can migrate to verifiable rules is the watershed between on-chain monetary competition and classical banking competition.

Both systems face the latent conflict that "rule-makers are also rule beneficiaries." Central-bank decision-makers face employment politics; core protocol teams holding large tokens face price incentives. The key is not which is cleaner, but whether constraint mechanisms can be externally observed and assessed. On-chain protocols offer stronger observability on some dimensions (contract code, public on-chain data) and remain immature on others (governance attacks, missing legal accountability).

In the popularization frame, Tokenomics lets small teams and individual developers design monetary-issuance and incentive experiments, with rapid market feedback on success or failure. That is an important expression of falling participation thresholds: no central-bank license is needed to issue a monetary unit; no investment-bank credentials are needed to design rate structures. Rapid feedback also means rapid punishment—badly designed Tokenomics can zero a protocol within months. Quality screening cannot be skipped; only the screening agents and mechanisms differ from the traditional system.

Section 7. Anatomy of Design Failure: Typical Case Types

Tokenomics failure types often illuminate design boundaries better than success cases. Several typical patterns deserve comparison.

Useless-token cash-outs: projects issue tokens with no real utility in the ecosystem; core functions work without holding the token. Tokens are pure financing tools. Such projects pump on stories in bull markets and zero quickly in bears; their Tokenomics never had long-run value support from the design stage.

Over-issuance inflation death spirals: excessive annualized rewards require continuous token issuance far faster than protocol value growth. Prices fall from oversupply; the dollar value of rewards shrinks; participants exit before rewards shrink further; liquidity contracts suddenly; prices fall further. Defective designs are often rapidly weeded out in bears, resources migrating to healthier incentive structures—Chapter 12's ICO clear-out already showed similar market screening; the full condition-consequence chains for Terra/UST and Anchor appear in Section 9 and Chapter 12, Section 5. This was the most common death path in the 2021–2022 DeFi bear market.

Governance attacks: attackers borrow large amounts of governance tokens, propose, pass, and withdraw within the same block—"flash-loan governance attacks." Beanstalk lost nearly \$180 million to such an attack in 2022, exposing the lack of defenses against large one-shot votes.

Oracle manipulation: lending protocols that rely on on-chain price oracles, if oracle sampling liquidity is thin, can be temporarily manipulated, collateral wrongly overvalued, large assets borrowed and withdrawn, leaving the protocol with bad debt. Such attacks often target newly listed, thin-liquidity token markets.

Most of these failures stem from incomplete attack-surface consideration at design time—they are not unpreventable. Robust Tokenomics needs coordinated incentive analysis, game-theoretic modeling, and security audit—not handing technology, economics, and security to three non-communicating teams.

Section 8. Staking Economics: Locking as a Long-Term Trust Mechanism

At a finer incentive-design level, staking deserves separate discussion. The basic logic: holders lock tokens into the protocol, perform specific functions (validating transactions, providing liquidity, acting as a safety buffer), and receive protocol rewards. Locking itself creates a time constraint: tokens cannot be sold during the lock—this “skin in the game” changes incentive structure—participants now care more about long-run protocol health because short-run cash-out is impossible.

Proof-of-stake (PoS) networks are the most complete realization of staking economics. After Ethereum’s PoS transition, validators must stake 32 ETH, validate blocks, and face substantial slashing of stake for dishonest behavior (double-signing, etc.). This “violators lose collateral” design maintains an honest equilibrium without centralized authority—validators’ rational choice is honesty, because expected validation rewards are far smaller than slashing losses.

Liquid staking further optimizes staking economics. Traditional staking requires locks during which tokens cannot be used—a liquidity loss. Protocols such as Lido and Rocket Pool accept user ETH stakes and issue equal staking receipt tokens (e.g., stETH); holders can use these receipts in DeFi while continuing to accrue staking yield. In substance this allows “one asset, two uses,” sharply raising capital efficiency, but also introduces extra depeg risk—in June 2022 stETH traded at roughly a 7%–8% discount to ETH on the secondary market, reflecting panic-period redemption queues combined with composability risk¹¹.

Openverse blue papers place Bitgold staking alongside PCIM issuance and VRC-12 enterprise staking of Bitsecurity as a core parameter layer: when staking ratios, lock periods, and slashing designs land as in the white paper, they will directly shape ecosystem expansion boundaries—before production one should not assert that “the monetary system’s governance core is already closed.”

Section 9. Cross-Protocol Incentive Composability and Systemic Risk

A distinctive DeFi feature is “composability”: tokens and positions across protocols can nest into complex value combinations. A user may stake ETH in Aave for an aETH receipt, place aETH in a Curve pool for Curve LP tokens, then stake LP tokens in Convex for extra rewards. Along the whole chain, each layer provides its own incentive tokens—and each layer introduces new risk.

Composability created dazzling yield stacking in bull markets and unpredictable cascade risk in stress events. When one protocol fails (e.g., Curve oracle attack or large Aave liquidations), all dependent positions face chain effects. The 2022 Luna/UST collapse’s impact on Anchor transmitted rapidly across DeFi—stepwise death-spiral mechanisms, cross-chain contagion, and the algorithmic-versus-overcollateralized spectrum.

Assessing a token’s Tokenomics risk cannot look only at that protocol’s design; one must map connection points to external protocols: which protocols depend on this token as collateral? Which oracles price it? Which external protocols correlate with this protocol’s reserve assets? That is the dimension of “Tokenomics ecosystem-graph” analysis—invisible at the single-protocol level, requiring assessment across the whole DeFi network.

If Openverse VRC protocols achieve composability with broader DeFi (e.g., Bitgold accepted as external collateral), they can by design gain stronger network effects and simultaneously inherit broader systemic-risk transmission—a strategic trade-off that must be tested with ecosystem-graph data, not extrapolated from roadmaps as a proven advantage.

The UST/LUNA collapse showed that high-APY stablecoins cannot maintain pegs long. Anchor-style “stablecoin deposit subsidies paid by token inflation” belong in Tokenomics as a variant of the over-issuance

inflation death spiral, unrelated to PCIM¹². Cong, Li & Wang (2024) formalize Anchor-style subsidies in a dynamic adoption model: when incentive release persistently exceeds real protocol yield, large holders exiting before retail is a rational equilibrium, not mere “market panic”¹³. The stepwise death-spiral chain (Liu et al. 2023; Brunnermeier et al. 2022) is detailed earlier; here only the boundary directly relevant to this chapter’s Tokenomics assessment: when the stability layer is algorithmic undercollateralization + high-yield subsidy, governance transparency cannot reverse mechanism-category error. Overcollateralized CDPs (such as VRC-10/PCIM, current tier $C_0 > 100\%$, upper tier near 161.8%) under shock follow the main path of coverage $C(x)$ falling and redemption runs—not infinite native-token issuance to fill gaps. The VRC-11 private-domain layer uses 61.8% undercollateralization, with structural gap $g(0) = 38.2\%$ from the first mint moment, requiring whitelist, off-chain redemption, and emergency reserves—cannot apply the public-domain $> 100\%$ standard. Both stability layers jointly obey: (1) must not rely on native burn/mint alone to absorb depeg pressure; (2) must not use unsustainable token issuance to maintain high deposit yields. Assessment must first classify the stability-mechanism spectrum: algorithmic, partially collateralized, and overcollateralized CDP types must not be conflated—Clements (2021), before Terra’s collapse, already traced algorithmic fragility to the historical uncontrollability of demand, arbitrage, and feed-price conditions, forming an ex-ante–ex-post contrast with Cong et al. (2024)’s Anchor-subsidy dynamic model¹³¹⁴. Even when red lines are observed, cross-protocol composition (above in this section) may still import UST-style risk indirectly as “reserve assets”—ecosystem-graph analysis cannot be completed by a single protocol alone. Open questions remain: DeFi composability means “single-protocol red-line compliance” is not “system immunity”—full-graph audit is required, not white papers alone. Death-spiral mechanisms; peg upper bounds and cross-protocol risk.

Section 10. Participation Thresholds and Sustainable Incentives

Assessing Tokenomics must ask simultaneously whether incentives can persist, whether supply matches demand, whether governance has anti-capture arrangements, and whether compositional risk enters design. For Openverse, when VRC-10 (Bitcurrency), VRC-11 (Privcurrency), and VRC-12 (Bitsecurity) share a Bitgold collateral pool, release curves, governance timelocks, and cross-protocol exposure must be checked item by item under the above framework—before production this is only design comparison, not a substitute for on-chain audit.

ERC-20 solves “how to interoperate”; Tokenomics solves “why anyone keeps using”—both equally important. Standard diffusion only lowers technical thresholds; sound incentive design brings long-run retention and value co-creation.

Even the cleverest incentive design, if ordinary users cannot understand how to participate, attracts only a few professionals. Unpredictable gas fees, cumbersome multi-step operations, steep private-key management—these frictions largely limit DeFi’s participation range. Account abstraction, gasless transactions, seamless wallet login, and related technologies are bridging the experience gap between professionals and ordinary users. If Openverse VRC access-layer experience meets design goals, it may lower popularization frictions—product data must test this; white papers must not extrapolate that “the idea has already become reality.”

The hard standard for assessing Tokenomics is whether it can maintain a participant base across a full economic cycle (including bull and bear markets) and deliver reasonable returns to honest long-term holders. Designs that fail this test are fleeting no matter how polished the white paper. One deeper meaning of popularization is that participants can use this chapter’s framework to assess the protocols they join, rather than blindly trusting issuer narratives.

Tokenomics' s core tension is temporal: short-run incentives often conflict with long-run system health. Individual rationality (enter at high rewards, exit at peaks) can aggregate into collective self-destruction—an on-chain variant of the tragedy of the commons. In *A Tract on Monetary Reform*, Keynes warned: “In the long run we are all dead”—economists who only announce that the ocean is flat again after the storm has passed are of no help to present policy choice¹⁵. On-chain design must encode property rights, use rules, and constraints on over-use in code; that is far harder than writing a white paper—and far more important.

注释与引用

1. Ethereum Foundation, "The Merge," 2022; Ultrasound.money post-Merge ETH annualized issuance ~0.5% (PoS) vs ~4% pre-Merge (PoW including block and uncle rewards). <https://ethereum.org/en/roadmap/merge/> ; <https://ultrasound.money/> ↩
2. DeFi Llama TVL historical series (same source as Chapter 5, Section 2 [^9]): early 2020 ~\$1 billion → November 2021 peak above \$180 billion → end-2022 below ~\$50 billion. <https://defillama.com/> ↩
3. Keynes, 1936, *The General Theory of Employment, Interest and Money*, Ch. 12: “Most, probably, of our decisions to do something positive ... can only be taken as a result of animal spirits—of a spontaneous urge to action rather than inaction, even though as the basis of rational calculation ... the motives for action might not be present.” Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩
4. Messari, "State of Crypto: Token Unlocks 2022": many 2021-issued projects drew down more than 90% from peak in the 2022 bear; CoinGecko 2022 annual report similar findings. <https://messari.io/report/state-of-crypto-token-unlocks-2022> ↩
5. Werner & Papadatos (2023), *IEEE Access* 11: flash-loan governance-attack taxonomy; Beanstalk 2022 governance attack loss ~\$180 million (on-chain flash-loan borrow-vote-withdraw); MakerDAO Endgame Litepaper (2023-03, source: official Litepaper v1, not independently audited): SubDAO split and MKR restructuring, post-Black Thursday evolution of liquidity modules such as D3M. <https://beanstalkfarms-almanac.medium.com/beanstalk-farms-governance-exploit-post-mortem-847a8566923e> ; <https://endgame.makerdao.com/> ↩ ↩²
6. Aquilina, Matteo, Sirio Aramonte, Patrick Bisias, Andreas Schrimpf, and Alexander Kothe. "The market structure of stablecoins." *BIS Bulletin* No. 73, 7 February 2023: issuance concentration, governance voting-power concentration, and run contagion aligned; Werner & Papadatos (2023), *IEEE Access* 11: governance-attack taxonomy. <https://www.bis.org/publ/bisbullet73.htm> ↩
7. Ultrasound.money: EIP-1559 base-fee burn and PoS issuance day-by-day net; high-gas months in 2022 saw net negative issuance. <https://ultrasound.money/> ↩
8. Keynes, 1936, *The General Theory of Employment, Interest and Money*, Ch. 15 and surrounding chapters: the central bank' s function of injecting liquidity into the financial system through open-market operations and maintaining the payments system in panic. Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩
9. Hayek, 1976, *The Denationalization of Money*, Ch. 12 “Which Currency Will the Public Select?,” p. 131: “Good money can come only from self-interest, not from benevolence.”; p. 23: inferior issuers “at once lead to the rapid displacement of the offending currency by others.” PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
10. Selgin, George, "The Evolution of a Free Banking System," *Economic Inquiry* 22(3), July 1984, pp. 289–300 (endogenized clearinghouse discount-reflux discipline); White, Lawrence H., *Free Banking in Britain* (1995), ch. 4 (clearing networks). <https://doi.org/10.1111/j.1465-7295.1984.tb00123.x> ↩
11. Kaiko Research, "The stETH Depeg" (June 2022): peak secondary-market stETH/ETH discount ~7%–8%, linked to Celsius and related redemption pressure and composable positions. <https://www.kaiko.com/research> ↩
12. Anchor Protocol White Paper (2020, source: official white paper, not independently audited): 20% UST deposit APY subsidized by ANC tokens. Buttman, Klemm & Pimma (2019), ECB OP 230: algorithmic vs fiat-/crypto-collateralized classification; Klages-Mundt et al. (2023), *Journal of Financial Stability* 68, 101142: stablecoin risk taxonomy and Terra

class algorithmic model boundaries. <https://anchorprotocol.com/docs/anchor-v1.pdf> ; <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230d57946be3b.en.pdf> ↩ ↩²

13. Cong, Lin William, Ye Li, and Neng Wang. "Tokenomics: Dynamic Adoption and Valuation." *Journal of Financial Economics* 151, 2024, pp. 103745: unsustainability of Anchor-style subsidies and sophisticated-first exit; Momtazi (2022), *Journal of Risk and Financial Management* 15(11), 520: post-mortem triple-failure survey of Terra/UST; Catalini, Goren & Shah (2021), MIT Sloan RP "Some Simple Economics of Stablecoins": algorithmic subsidy boundaries. <https://doi.org/10.1016/j.jfineco.2023.103745> ↩ ↩²
14. Clements, Ryan (2021), "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins," *Wake Forest Law Review Online* 11, 131–171 (algorithmic triad: baseline demand, arbitrage participation, reliable feeds; pre-Terra monograph). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3952045 ↩
15. Keynes, 1923, *A Tract on Monetary Reform*, Ch. 3: "In the long run we are all dead. Economists set themselves too easy, too useless a task if in tempestuous seasons they can only tell us that when the storm is long past the ocean is flat again." Project Gutenberg: <https://www.gutenberg.org/ebooks/32637> ↩

§ 14 Public Currency and PCIM

30-second version of this chapter: For public currency to serve on-chain as a “near-fiat constant-value unit,” there must be publicly testable issuance discipline—this book calls it PCIM (Public Currency Issuance Mechanism). The abstract mechanism is: overcollateralization with volatile collateral, mint/redeem same-price arbitrage, and circulation-threshold public votes adjusting tightness; no Maker-style liquidation auctions—extreme markets run through redemption and reserves. In the Openverse white paper, VRC-10 (Bitcurrency) and Bitgold (BTG) are one engineering instance of PCIM; formulas and tier tables below describe the general mechanism; Openverse mappings appear in each section’s “implementation sample.”

Tokenomics answers “why anyone keeps using”; public settlement must land incentive constraints on a mortgageable, redeemable constant-value unit. This chapter first states the PCIM abstract mechanism (Sections 2–3 and Section 9’s minimal model), then uses Openverse / VRC-10 to illustrate one landing path; cited Bitgold white-paper (v2.1.5) clauses are executable statements of that instance, not verified conclusions. The path differs from simple pegs of centralized stablecoins and from CBDC state-backed issuance. The Bitgold white paper summarizes the overall experiment in three steps: public-currency operating platform, digital-asset self-governance architecture, distributed economic ecosystem—this chapter focuses on the first step’s core mechanism; evolution path and cross-ecosystem interoperability appear in Section 10.

Section 1. Bitcurrency’s Positioning and Naming

On-chain stablecoin market caps exceed hundreds of billions of dollars; nominal transfer volumes often exceed Visa’s traditional payment network—yet the gap between nominal flow and real payment definitions is enormous (three definitions in Chapter 1, Section 8)¹. Extrapolating from nominal transfers that “the public settlement layer has already displaced fiat monopoly at scale” conflates technical traffic with institutional adoption—on-chain settlement is highly active in DeFi and crypto pairs, but retail wages, tax, and public finance still price in domestic currency. The present pattern shows significant demand for verifiable, composable settlement units; reserve transparency and redemption still depend on centralized issuers’ audits. PCIM tries to upgrade “verifiable reserves” from institutional promise to protocol state—whether comparable adoption appears outside any one ecosystem must be tested by adjusted payment growth, peg-deviation panels, and corridor penetration—not by roadmap presumption alone.

Public currency (Bitcurrency) under the PCIM frame means: a constant-value asset minted through overcollateralization of on-chain volatile collateral (Bitgold in the Openverse instance), namable against concrete fiat units (e.g., dollar units), and serving a settlement role within open ecosystems. That naming—fiat units for on-chain assets—has both practical motives and conceptual ambition.

The practical motive: for most users, pricing in familiar currency units sharply lowers cognitive friction. If Bitcurrency-USD’s purchasing power within an ecosystem is statistically near the dollar, users need not continually convert; settlement experience approaches card spending. That is the main reason stablecoins rapidly penetrated cross-border payments, OTC trading, and DeFi clearing in recent years—lower cognitive burden, higher usability.

The conceptual ambition: Bitcurrency deliberately draws a line against USDT-class centralized stablecoins. The latter’s value stability depends on the issuer (Tether) holding adequate dollar reserves and promising on-demand redemption—essentially the issuer’s liability certificate. The former stresses public-domain rules and multi-agent participation—issuance depends on on-chain verifiable collateral state and mint/redeem rules, not a

single institution’ s credit and promise. Spiritually this continues Hayek’ s critique of fiat monopoly and advocacy of monetary competition, but the path is entirely different: Hayek envisioned private banks freely issuing competing currencies; PCIM walks a unified public-domain protocol frame in which multiple agents participate under the same rules.

Analogizing Bitcurrency to an on-chain competitor of M0 (cash in circulation) helps grasp its positioning ambition. M0 is the monetary system’ s base layer—direct central-bank liability, highest liquidity and widest acceptance. If Bitcurrency can play a similar role within open ecosystems—as the settlement base unit for other on-chain financial activity—it is replicating M0 function at the protocol layer. **Implementation sample (Openverse):** the white paper (v2.1.5) describes public currency as “fiat’ s representation in the blockchain world,” a bridge between the trust economy and mainstream economies, and self-compares to M0—its target is constant-value public assets encoded under the VRC-10 standard for each sovereign fiat unit, not competing with USDT as the same product form of centralized stablecoin. USDT is a private institution’ s liability certificate, depending on Tether’ s reserve promise and audits; the Openverse instance stresses competitive issuance overcollateralized with Bitgold and on-chain verifiable collateral state. That distinction is clear in marketing and blurrier in regulatory classification—legal uncertainty discussed earlier in this book.

Implementation sample (Openverse): the mainnet embeds 200-plus fiat-unit public currencies referencing ISO 4217 (USD, CAD, CNY, JPY, INR, etc.), extensible further at the protocol layer. Unlike the simplified narrative of “only one dollar stablecoin on-chain,” this is closer to Hayek’ s vision of multiple parallel currencies—except competition units shift from nineteenth-century private banknotes to collateralized issuance quotas under a unified interface (VRC-10); superiority is still decided by holders’ and merchants’ voting with their feet.

Global fiat mapping gains operational meaning here: ISO 4217 supplies the sovereign symbol table; the public-domain interface standard (VRC-10 in Openverse) supplies on-chain composable, auditable parallel representations—each fiat unit admitted to the standard corresponds to a named Bitcurrency, mapping accounting symbols and purchasing-power targets, not overnight abolition of national legal tender. Domestic tax and retail may still lock to local currency; mapping first accumulates adoption in cross-border, open-ecosystem, and high-friction scenes. The global mainstream circulating medium means only public-layer Bitcurrency (VRC-10 in Openverse), excluding VRC-11 Privcurrency.

Minting as choice jointly with mapping: under PCIM, participants meeting collateral conditions stake collateral (Bitgold in the Openverse instance) and mint or redeem Bitcurrency at the currently effective tier’ s collateral ratio (tier mechanism in Section 2.2); every expansion or contraction is an economic choice, not administrative rationing. Choosing to lock BTG as collateral for public circulating positions, or contracting supply through redemption channels—discipline is written in the on-chain state machine, readable by third parties. Minting as choice does not guarantee “good money always wins”; it only raises competition frequency and transparency to block-time scale; dynamics of weeding-out and convergence of the global circulating layer follow later.

But analogy boundaries must be watched: fiat M0 is backed by the entire central-bank–commercial-bank credit system and legal forced acceptance. On-chain public currency must win adoption and compliance space on its own—an institutional and market challenge beyond technical standards.

Section 2. PCIM’ s Operating Logic: Protocolizing a New Gold Standard

PCIM can be read as a protocolized realization of “new gold standard” thinking. The gold standard’ s core logic: monetary issuance constrained by gold reserves; gold as an exogenous value anchor preventing political overissue. That system was abandoned in the twentieth century for inability to respond flexibly to economic crises

and war finance, yet its pursuit of supply discipline remains a reference point in economic discussion. Every major innovation in money and banking accompanies dissolution of old structures and reconstruction of new credit relations—Schumpeter systematically traces this in *History of Economic Analysis*².

PCIM takes on-chain volatile collateral as reserve anchor (Bitgold in the Openverse instance) and designs a “stake-to-borrow” issuance path: eligible participants stake collateral and, at protocol-specified collateral ratios, borrow corresponding Bitcurrency. Structurally this resembles traditional banking credit creation—banks accept deposits and lend at higher multiples, creating new money—but PCIM’s critical difference is that collateral state and issuance quantity are on-chain verifiable, not numbers hidden in commercial-bank balance-sheet back offices.

Concrete mechanisms involve several key parameters that must align with the VRC-11 private layer and terminology below. Collateral ratio C_0 (collateral market value ÷ debt face value) and mint yield σ (debt face value as a share of collateral market value) are reciprocals: $\sigma = 100\%/C_0$. The public layer (VRC-10 in Openverse) does not set MakerDAO-style liquidation lines (L) or warning lines (W)— C is for monitoring only and does not trigger on-chain forced auctions; stability depends on mint/redeem arbitrage, protocol reserves, and circulation-triggered tier public votes (see Section 2.2). Second is oracle pricing: mint and redeem both execute against on-chain consensus quotes for collateral. The VRC-11 private layer uses 61.8% undercollateralization parameters, likewise no liquidation/warning lines; risk control layers enterprise reputation, whitelists, and off-chain redemption—not participating in public-tier mechanisms.

“Popular” appears in decentralized issuance rights: those who press the issue button are no longer only central banks, but multiple agents staking and borrowing under public rules, jointly constituting money supply. Technically, any address holding enough collateral and meeting protocol conditions may participate. Whether broad participation is truly reached depends on three constraints: collateral liquidity and availability (if highly concentrated among early participants, decentralized issuance rights are only appearance); interface usability (contract interaction still has technical barriers for most ordinary users); and regulatory attitudes across jurisdictions (if participating in money-like issuance is treated as operating unlicensed money business, most potential participants will hang back). Technology supplies possibility; institutions decide reality—whether protocols land ultimately depends on liquidity, compliance, and judicial recognition, not code alone.

Implementation sample (Openverse) summarizes PCIM competitive-issuance operating points in six items: holding Bitgold suffices to participate (eligibility tied to collateral, not bank licenses); overcollateralization generates public currency; unlocking collateral contracts supply; design aims for issuance paths without interest or fees; enter and exit anytime without waiting for monetary-policy-committee cycles; issuance rhythm uses block time as scale so money creation is near-real-time observable; public currencies collectively cover fiat units and possible future public asset classes. From this it asserts: cross-border choosable public-currency competition will attract long-term holding to units of more stable purchasing power and squeeze inferior sovereign fiat’s circulating space—“good money drives out bad” expanding from domestic legal-parity scenes to cross-sovereign comparison. That logic continues Thiers’ law, but reality still depends on liquidity depth, compliant access, and clearing infrastructure; protocol proclamations alone cannot self-realize. How mismanaged fiat and its on-chain mappings weed each other out under parallel competition, and how the global circulating layer converges on a few mappings, appears later in discussions of inferior-money exit and reserve–circulation division of labor.

Section 2.2 Dynamic Mint Yield: Circulation Tiers and Public-Vote Gates

Breathing note: the following section is the book’s most technical, but the question itself is intuitive—as more dollar stablecoins circulate, can the community vote to let “the same collateral mint more face value”? Yes,

but only by public vote; if the vote fails, rules stay; crises can also open separate votes to tighten (require more collateral). Formulas stay in the table; Openverse' s Bitcurrency-USD four-tier figures are a reference instance.

PCIM' s collateral discipline is not a book-wide single "initially 161.8%" constant, but a dynamic mechanism tiered by each public mapping' s circulation and confirmed by public vote—in Openverse applying only to the VRC-10 public layer; VRC-11 private-domain stablecoins do not participate in this tier table.

Mint yield σ is defined as: Bitcurrency face value mintable per 1 unit of Bitgold market value as a share of collateral value (reciprocal of collateral ratio). Lower σ means more BTG must be staked to mint equal face value—the system is more conservative; higher σ lets each BTG mint more stablecoins—expansion elasticity rises and systemic risk rises in parallel. The protocol uses each mapping' s independent circulation S (e.g., Bitcurrency-USD' s on-chain circulating face value) to trigger dynamic-ratio public votes: at thresholds, governance votes auto-trigger to consider switching to the next σ ; if the vote fails, the current-tier stake ratio is maintained unchanged—this is the core risk gate, not silent loosening the moment circulation arrives.

Bitcurrency-USD reference tiers (Openverse instance; other fiat mappings or other-chain deployments may configure different thresholds and ratios, same principle):

Circulation S threshold	Mint yield σ under vote	Equivalent collateral ratio $C_0 = 100\%/\sigma$
1 million USD	23.6% (0.382×0.618)	$\approx 424\%$
10 million USD	38.2%	$\approx 262\%$
100 million USD	50%	200%
1 billion USD	61.8%	$\approx 161.8\%$

The table' s 61.8% yield corresponds to collateral ratio about 161.8%—the upper tier of the ordinary upgrade path (excess buffer $\sim 61.8\%$), not an initial parameter applying from small scale. At early low circulation, σ is lower and C_0 higher—more conservative in the experimental stage; only community approval in public votes allows entry into higher-yield tiers with scale.

Crisis tightening: the upgrade path has an upper bound but no lower bound. Under collateral plunges, redemption runs, or sustained peg deviation, governance may separately initiate votes to raise C_0 (lower σ) — e.g., from 61.8% yield back to 50% or lower—to shrink marginal expansion elasticity and require new mints to bear thicker collateral. Same direction as Maker raising ETH minimum collateral ratios after "Black Thursday," but via split-track quorum + timelock explicit votes, not closed-door ex-post parameter changes. Upgrade and downgrade on split governance tracks avoid single-block flash passage of "cut collateral in chaos" during crises.

Mint and redeem share the same effective tier' s σ and oracle definitions, preventing "high-mint, low-redeem" split. Tier state, threshold progress, and vote results should be on-chain readable so regulators and holders need not wait for quarterly reports to observe "how tight current discipline is."

Contrasted with Terra/UST-style crises of unilateral expansion and Anchor high yields pulling deposits: PCIM' s expansion elasticity is bound to circulation milestones + public-vote approval; if votes fail, discipline is unchanged. Risk relies not on liquidation auctions but on three stacked layers—conservative starting tiers, upgrades requiring democratic confirmation, crises allowing public-vote tightening—still requiring mainnet stress data, not white-paper promises.

Section 3. Economic Robustness of Collateralized Issuance

PCIM depends on collateral value support. Under normal markets, Bitgold's value exceeds borrowed Bitcurrency face value—the system is safe. When Bitgold prices fall, collateral value declines and coverage thins, but VRC-10 does not set MakerDAO-style liquidation thresholds—participants may voluntarily add collateral or redeem Bitcurrency to unlock Bitgold; the protocol may also circuit-break and pause new mints and deploy reserves to support redemption channels.

A risk to face squarely comes from MakerDAO and similar CDP protocols: when collateral ratios breach set thresholds, forced liquidation sells collateral on the market—March 2020 “Black Thursday” showed that automatic liquidation itself can amplify declines into liquidation cascades. PCIM deliberately avoids that path, but Bitgold plunges may still trigger redemption runs (participants concentrate on redeeming Bitcurrency to unlock BTG) and secondary depeg—not on-chain auction cascades. Without enough design-level buffers for black swans (C_0 , reserves, issuance caps), the public peg is equally stressed.

Liquidation cascades and oracle failure. Under MakerDAO-style $C < L$ triggering on-chain forced auctions, collateral dumping can amplify price declines and push more positions below L —March 2020 ETH intraday drops ~30%+, zero-price auctions, and DAI premiums are empirical benchmarks; Qin et al. (2021) longitudinal liquidation data on Maker/Aave/Compound/dYdX show existing designs incentivize liquidators yet often oversell collateral at steep discounts at borrowers' expense³. VRC-10 deliberately sets no L/W , so the main pressure path becomes redemption runs rather than auction cascades—when redemptions synchronize with VRC-12 liquidations and VRC-11 redemptions, BTG faces combined “unlock sell pressure + auction sell pressure.” If oracles on thin pools are flash-loan manipulated instantaneously, wrong feeds can complete over-minting before circuit breakers—Chitra & Angeris (2020) show TWAP windows must be jointly designed with pool depth; Aramonte et al. (2021) BIS post-mortem notes that under DeFi's “decentralization” appearance, oracles, governance, and liquidity remain highly concentrated—verifiable $\neq$ de-risked⁴. When CEX and DEX liquidity quality split (Barbon & Rinaldo 2024), mint/redeem arbitrage chains fail under gas fees and insufficient cross-venue depth; δ upper-bound models must include OTC/DEX segmentation in scenario assumptions rather than default to a single continuous market⁵. Avoiding liquidation cascades does not eliminate systemic risk—redemption queues may be slower and less predictable when liquidity dries; Aspris (2024) empirics on Maker vault-level leverage also show over-leverage especially harms low-skill participants—whether PCIM three-chain closure holds under extremes must be tested against stress data and Maker-class CDP depeg events (S&P Global 2023; Chitra et al. 2024 DAISIM), not white-paper promises alone.

PCIM parameterizes robustness as the white paper envisions: currently effective tier C_0 and σ (upgrade ceiling ~161.8% collateral / 61.8% yield; see Section 2.2); protocol reserves absorbing gaps under redemption pressure; issuance-size caps on single collateral types. MakerDAO historically adjusted collateral ratios through governance many times—PCIM does not copy its liquidation-line design, but must combine circuit breakers, reserves, and tier public votes.

These parameter combinations have MakerDAO, Aave, and other DeFi precedents; if PCIM, as the white paper envisions, fully implements on-chain circuit breakers, reserves, and mint/redeem same-price, it has a robustness hypothesis comparable to similar overcollateralized CDPs—pending mainnet stress data and independent audit. If those mechanisms have design blind spots or are unimplemented, severe deviation of Bitcurrency from its nominal anchor (e.g., the dollar) may appear under stress, damaging user confidence and system credibility.

Beware the leap “overcollateralization + no liquidation line = immunity to extremes”: March 2020 MakerDAO “Black Thursday” showed forced liquidation can amplify declines; though PCIM avoids liquidation cascades, it still faces redemption runs and bad feeds—full derivation in Section 9’ s minimal model.

Section 4. Triangular Comparison with Stablecoins and CBDC

To position Bitcurrency and PCIM, first see three main forms in the current monetary-technology landscape—centralized stablecoins, CBDC, and decentralized collateralized stablecoins—each with different trust bases and risk structures.

Centralized stablecoins (USDT, USDC): value stability depends on issuers’ reserve transparency and redemption promises. Core risk is counterparty risk—if reserves are inadequate, the issuer fails, or regulators freeze, holders may not redeem in full. Advantages are simple operation, scalable size, and smooth docking with existing banking. Regulation focuses on reserve-asset quality and audit transparency, and license qualifications.

Central bank digital currency (CBDC): direct digitalization of fiat, issued by the central bank as direct liability to holders. No counterparty risk (within sovereign credit), with legal-tender status and forced acceptance. Risk concentrates on privacy surveillance and monetary-policy transmission—central banks can micro-operate money supply on individual CBDC accounts, policy-wise double-edged: precise policy or abuse as financial-censorship tools⁶. Brunnermeier and Niepelt (2020) under an equivalence framework note that how CBDC is introduced determines whether it rewrites bank liability costs and fiscal-monetary borders; Bindseil’ s tiered design (payment-type vs investment-type) is most central banks’ institutional response trying to limit CBDC to “cash extension” rather than “store-of-value competing with Treasuries.”

Decentralized collateralized stablecoins (DAI, and Bitcurrency’ s design positioning on the overcollateralization dimension): value support from on-chain verifiable overcollateralization, no single issuer. Advantages: strong censorship resistance, high transparency, good DeFi composability. DAI and similar CDPs’ core risks include collateral-price volatility and liquidation cascades; Bitcurrency (VRC-10) deliberately sets no liquidation/warning lines, so core risks become redemption runs, reserve exhaustion, and governance capture leading to malicious parameter changes. Lyons & Viswanath-Natraj (2020) show that even USDC-class fiat-collateralized stablecoins’ pegs depend on reserve redeemability and OTC depth, not reserve statements alone⁷; Griffin & Shams (2020) empirics on Tether reserves likewise show fiat-collateral transparency controversies can shock pegs⁷.

If in crisis governance proposes cutting C_0 , unilaterally expanding, or using public reserves to “fill gaps” (Maker’ s ex-post parameter revisions; Terra #1623 deploying LFG BTC reserves are precedents), “verifiable rules” become empty under capture—split-track quorum, maximum-delay timelocks, and voting-power warm-up are required. Under high concentration, constraints may still be eroded in stages; on-chain democracy in crisis still reacts slower than central-bank midnight coordination. Governance capture is another risk layer. Parameter transparency does not automatically equal capture resistance—crisis proposals to cut collateral ratios or emergency unilateral expansion have precedents in Maker and Terra governance history. PCIM parameter changes therefore need debatable engineering constraints: timelocks (markets can react), multisig/segmented quorum (flash-loan single-block passage infeasible), split-track governance of collateral parameters and the “competitive-issuance switch,” crisis pause allowing only additional collateral and redemption rather than unilateral expansion—verifiable rules must include “rules for changing the rules.” Under high concentration, those constraints may still be eroded by long lobbying or staged passage; protocols cannot replace courts holding malicious governance accountable—an unsolved gap between on-chain democracy and the rule of law.

Governance capture stacked with death spirals (Terra contrast). When UST depeg triggered community proposals to deploy Luna Foundation Guard BTC reserves for a “bailout” (May 2022 proposal #1623 etc.), governance in substance tried unilateral expansion / use of public reserves to fill algorithmic gaps—contrasting PCIM’ s engineering constraint forbidding unilateral expansion in crisis. Even passed votes could not stop LUNA supply explosion and UST zeroing, showing: transparent governance $\neq$ effective governance; when the stability mechanism itself is algorithmic undercollateralization, even perfect quorum can only delay rather than reverse death spirals. Maker after “Black Thursday” raised ETH collateral ratios through governance and introduced D3M, showing PCIM must accept: C_0 must be used jointly with ex-post governance revision—ordinary upgrades via circulation-threshold public votes; crises may also vote to raise collateral ratios and lower yields to tighten discipline (Section 2.2). One-time parameter setting is not permanently safe. Split-track quorum and timelocks under high concentration may still be eroded in stages; on-chain democracy in crisis still reacts slower than central-bank midnight coordination; Terra shows governance capture and mechanism-category error can stack—PCIM’ s governance constraints can only constrain “how rules change,” not alone guarantee peg closure.

The VRC-10 path stacks public-domain protocol, collateralized issuance, and fiat-unit naming, forming unique design space but also unique regulatory-classification difficulty: is it a stablecoin? A deposit substitute? An unregistered security? Answers vary by jurisdiction and are still evolving in global regulatory practice. For participants, the key is identifying where risk hangs: smart-contract bugs, Bitgold market volatility, governance-level parameter-change rights, cross-border compliance duties. No single answer fits everyone; read protocol docs and on-chain implementations item by item, judging against one’ s own risk tolerance.

Section 5. Historical References for Parallel-Currency Experiments

In monetary history, multiple currencies circulating in parallel is not new. Before countries abandoned the gold standard, domestic banknote-issue competition, international gold–silver bimetalism contests, and parallel use of trade credit instruments were all historical forms of “parallel money.” Private banknotes briefly circulated in the nineteenth-century American free-banking era; competition’ s result was inferior banks failing and superior banks’ notes circulating at a premium—markets screening monetary quality by reputation⁸.

Contemporary on-chain monetary experiments spiritually echo that history, but the background differs: legal systems no longer allow private banks freely to issue directly circulating money; the global financial system is highly integrated; the importance of stability expectations far exceeds free-competition-era imagination. Even if Bitcurrency and fiat coexist long rather than substitute, the parallel experiment still has value: alternative units of account for cross-border settlement, infrastructure independent of traditional banking for open-ecosystem internal settlement, and pushing public and regulators to discuss whether “monetary issuance rules should be auditable and participable.”

Failed parallel-currency experiments equally educate markets. Collateral models’ actual behavior under extremes, friction costs of on-chain redemption, decentralized governance’ s crisis response speed—all must be tested in real markets, not only in simulators and white papers. Every controllable failure is tuition toward system maturity.

Section 6. Bitgold as Reserve Base: Szabo’ s Lineage and Protocol Parameters

PCIM’ s participability ultimately depends on Bitgold’ s availability and liquidity. If Bitgold’ s initial allocation is highly concentrated among early participants without effective redistribution, “popular issuance” in practice degenerates into “a few whales’ issuance.” No assertion is made here about Openverse’ s concrete

allocation—only questions that should be asked when assessing any issuance mechanism with a native token as reserve base.

Bitgold (BTG)’s naming and parameter design must be placed back in the intellectual-history coordinates the white paper sketches. In 2005, Nick Szabo proposed “bit gold”: using verifiable proof of work to create online “unforgeable scarce bits,” minimizing dependence on trusted third parties, and forming transferable scarce chains via distributed property registries and timestamps—an important precursor of Bitcoin thought⁹. Szabo’s 1997 “The God Protocol” already envisioned a verifiable third-party substitute where “God knows the outcome, humans can only verify”; 1999’s “Trusted Third Parties Are Security Holes” institutionalized the claim that money must turn to cryptographic constraints; 2002’s “Shelling Out” traced money’s cooperative origins from prehistoric collectibles—Nakamoto’s 2008 white paper §§1–2 embedded timestamp servers and PoW in P2P electronic cash; Finney’s 2004 RPOW was an engineering bridge between the bit-gold vision and Nakamoto’s chain⁹. Szabo’s 2017 “social scalability” further noted that blockchain money’s value lies in replacing interpersonal trust costs with verifiable rules—aligned with PCIM’s emphasis on “constraint carriers shifting from reputation to verifiable rules”¹⁰. Openverse’s white paper naming the native token Bitgold both honors that lineage and deliberately divides labor with Bitcoin’s occupied “digital gold” narrative: Bitcoin’s rigid supply, large price volatility, and limited on-chain throughput make it hard to carry daily payments; the white paper self-positions as, while inheriting decentralized ledgers and smart contracts, completing Bitcoin’s unfinished “peer-to-peer electronic cash” vision with constant-value public currency (official marketing copy says “Bitcoin 3.0”; this book cites it only as self-description, without independent evaluation).

At the protocol-parameter layer, Bitgold’s total is fixed at 200 million (the white paper analogizes to roughly 204,800 tons of historical gold extraction), with production halving every three years, and developers advised to prefer decimal expansion for subdivision needs rather than rewriting the total ceiling—spiritually near Bitcoin’s four-year halving and 21-million cap, with different parameters serving PoS staking and collateralized-issuance ecosystem rhythm. The consensus layer uses proof of stake (PoS); validators stake Bitgold to participate in block production and validation; in the classic safety–liveness–asynchrony trade-off, Openverse tends to prioritize safety—consistent with public currency’s settlement role, also meaning some liveness may be sacrificed under extreme network conditions.

The white paper has a highly binding statement on Bitgold’s function: “Bitgold has only one use—as the base asset for collateralized issuance of public currency.” Clarify exact meaning: “only one use” here means Bitgold’s monetary-economic use—it does not serve as a daily Bitcurrency-style payment medium; its main function is constraining VRC-10/11/12 collateralized issuance; this does not conflict with its simultaneous protocol-operation roles of POS staking (validators stake to produce blocks) and on-chain fee medium—the latter two are network-operation functions of any PoS native token, not another “monetary use.” On this reading, Bitgold is closer to gold’s on-chain recording and constraint layer in the gold-standard era: its price is market-discovered; public currency strives for approximately constant purchasing power under ISO fiat-unit naming. The white paper also envisions an extreme long-run scenario: if Bitgold prices stabilize long at high levels, public-currency issuance may shrink accordingly or even “disappear on its own,” and Bitgold itself might approach a global unified value scale—a fifty-year-scale thought experiment, recorded here without prediction.

Bitgold allocation sources usually include: team shares (typically locked), early-investor shares, community incentives, public sales, and ecosystem-building rewards. If the latter two classes are large and release rhythm reasonable, broad distribution is expectable. If the former dominate with concentrated unlocks, circulating Bitgold holding concentration needs continuous monitoring.

On top of broad distribution, Bitgold needs enough trading liquidity for ordinary participants to buy at reasonable prices. If Bitgold trades mainly on a few small exchanges with insufficient depth, large buys and sells cause large slippage, and the cost of entering PCIM collateral will exceed expectations. Listing on major exchanges, stable market-maker mechanisms, and adequate on-chain DEX liquidity are all necessary infrastructure conditions for PCIM truly to achieve broad participation.

Section 7. Regulatory Paths and Compliance Prospects

Any digital asset named against sovereign fiat units necessarily enters national monetary regulators' sight. In the US, draft regulation of dollar-pegged stablecoins has advanced in recent years, requiring issuers to hold adequate reserves, accept audits, and register with the Fed or OCC. In the EU, MiCA (Markets in Crypto-Assets) sets issuance thresholds and reserve requirements separately for "asset-referenced tokens" (ART) and "e-money tokens" (EMT). In China, any form of private stablecoin issuance is under strict restriction.

Bitcurrency as a "fiat-named token" issued by decentralized collateral mechanisms is unclearly classified under all these frames. That regulatory frameworks have not formed clear applicability paths does not necessarily mean illegality, but uncertainty itself is a risk factor—regulatory rulings may suddenly change a protocol's compliance status, affecting exchange listings, institutional participation, and cross-border use.

Responsible protocol design should preset compliance interfaces: optional compliance modules for KYC/AML at the technical layer; governance-level response mechanisms to regulatory change; legal-entity-level registration of foundations or other compliant bodies in jurisdictions with relatively clear token regulation. These arrangements cannot eliminate regulatory uncertainty but can maximize protocol survival capacity under regulatory change.

Section 8. Bitcurrency's Acceptance Network: Adoption Curves and Network Effects

Any money's ultimate value depends on the scale of people and scenes that accept it. Economics calls this money's network effects: more acceptors make holders more willing to hold, attracting more acceptors in turn—positive feedback. The dollar's lasting dominance comes in large part from decades of accumulated network effects—global commodities priced in dollars, most cross-border trade settled in dollars, central banks holding dollars as reserves, countless market participants holding dollars because they know others hold dollars.

For Bitcurrency to find survival space in this already highly competitive landscape, it needs a clear "acceptance-network launch strategy." Within the Openverse ecosystem, applications, service providers, and users form the initial acceptance circle—if Openverse Square's main participants default to Bitcurrency pricing and trading, in-circle acceptance is naturally established. The question is how to expand outside the ecosystem: which exchanges to partner with for circulation channels, which payment providers for use scenes, which enterprises to make Bitcurrency a procurement or payroll option.

Geographic expansion of acceptance networks must proceed in parallel with regulatory compliance. Accepting a foreign public currency in different countries usually requires local Money Service Business or equivalent licenses. That means Bitcurrency's cross-border promotion cannot rely on a single technical deployment but must complete independent compliance work in each target market, or partner with local compliant institutions already holding relevant licenses. This is threshold work, but the threshold exists fairly for any public currency seriously advancing compliant expansion—not an extra restriction aimed at Bitcurrency.

Application scenes listed in the white paper supply concrete handles for the above adoption curve: quote and settlement intermediary currency for DEXs within Openverse; supporting low-fee, near-real-time cross-border remittance and conversion (relative to traditional correspondent networks); docking face-to-face, App, and

website payments so merchant settlement enters unified on-chain clearing directly; and enterprise use cases such as smart-contract performance payments and payroll. The white paper says public currency “can infinitely expand capability in scenes where fiat can be used”—this phrasing is best read as a design ambition; in reality each scene class must pass local payment licensing, FX controls, and tax treatment. Bitcurrency’ s key difference from USDT is: the former, per white-paper design, puts issuance rules and collateral state on-chain; the latter institutionalizes reserve audits; merchants and users ultimately choose by comprehensive trade-offs among friction, compliance, and trust costs—not ideal-type lists in white papers.

Simultaneous contrast: real payment shares remain marginal (Chapter 1, Section 8)¹; Ma et al. (2023) show stress-period stablecoin flows highly synchronized with crypto-market liquidity¹; most advanced economies’ wages and taxes still lock to local currency. Even default Bitcurrency settlement within Openverse only constitutes local network effects inside a permissioned acceptance circle—outward expansion requires country-by-country payment licenses, FX compliance, and merchant onboarding, similar to USDC exchange listings and Circle reserve audits—not global adoption upon protocol deployment. Whether Bitcurrency can replicate USDT’ s OTC depth and redemption channels at the public layer still lacks adequate data; each deployment scene must separately meter penetration—cannot extrapolate from TVL or nominal transfers.

Section 9. Public Currency’ s Value-Stability Mechanism: Minimal Model and Stress Tests

If public currency is to perform settlement functions within an ecosystem, value stability relative to the nominal anchor (e.g., the dollar) is a hard constraint. Violent price swings make contract pricing difficult—if Bitcurrency-USD is worth \$1 today and \$0.8 tomorrow, any Bitcurrency-priced contract faces unacceptable value uncertainty. Prior sections stated PCIM mechanism points; C_0 takes the currently effective tier (dynamic tiers in Section 2.2), not a book-wide single constant. This section organizes them into a minimal computable model—comparative-static derivation under single-period isomorphic positions, closing the gap between “constant-value public currency + volatile collateral” into a computable, testable upper-bound function $\delta(x)$. Numerical examples below use the upper tier $C_0 \approx 161.8\%$ ($\sigma = 61.8\%$); other tiers plug into the same equations.

This section jointly derives peg-deviation upper bounds from three mechanism chains—oracle pricing, overcollateralization constraints, mint/redeem arbitrage; 38.2% in VRC-10 means BTG critical drawdown x^* , in VRC-11 the structural gap $g(0)$ from the first mint—must not be conflated with stake ratios; VRC-10/11 do not set Maker-style liquidation lines L / warning lines W ; under extremes the pressure path is redemption runs and reserve consumption. Given on-chain observed x and δ , one can reverse-infer which chain—arbitrage, reserves, or oracles—has failed.

Given BTG drawdown x , three-step computation of δ upper bound (upper-bound quick calc, not an operating promise):

Step	Operation	Judgment
1	$C(x) = C_0(1 - x)$	Post-shock collateral ratio
2	$g(x) = \max(0, 100\% - C(x))$; $x^* = 1 - 100\%/C_0$	$g = 0$ when $x < x^*$; gap positive when $x \geq x^*$
3	$x < x^* \Rightarrow \delta \leq \varepsilon$; $x \geq x^* \Rightarrow \delta \leq \varepsilon + \max(0, g(x) - R)$	Peg-deviation upper bound

Core symbol definitions:

Symbol	Definition	VRC-10 baseline
C_0	Currently effective tier collateral ratio (collateral MV ÷ debt face)	Upper-tier example 161.8%

Symbol	Definition	VRC-10 baseline
x	Bitgold drawdown relative to oracle reference price (0–1)	—
$C(x)$	Post-shock collateral ratio: $C(x) = C_0(1 - x)$	—
x^*	Critical drawdown where coverage breaks 100%: $x^* = 1 - 100\%/C_0$	$\approx 38.2\%$ (BTG price threshold, not stake ratio)
$g(x)$	On-chain collateral gap (share of debt face): $g(x) = \max(0, 100\% - C(x))$	—
ε	Mint/redeem arbitrage bandwidth (fees + slippage + delay)	Usually < 1%
R	Protocol reserves as share of circulating Bitcurrency	Scenario assumption
δ	Secondary-market price peg deviation from anchor	—
θ	Oracle single-block anomaly circuit-breaker threshold ($ \Delta p_{\text{block}} > \theta$ pauses new mints)	e.g. 20%
L/W	Liquidation line / warning line	Neither VRC-10 nor VRC-11 sets

Under the “oracle chain + collateral chain + arbitrage chain” three-chain closure frame, the core question is: given C_0 , x , ε , R , derive Bitcurrency deviation upper bound δ —given observed x and δ , reverse-infer whether arbitrage failed or reserves are insufficient; the model gives an **upper bound**, not an operating promise, and thus can be tested by mainnet data.

Model summary (one sentence): post-shock coverage $C(x) = C_0(1 - x)$; critical drawdown $x^* = 1 - 100\%/C_0 \approx 38.2\%$ (BTG price-shock threshold, not stake ratio); when $x < x^*$ peg deviation $\delta \leq \varepsilon$; when $x \geq x^*$ on-chain collateral gap $g(x) = \max(0, 100\% - C(x))$, deviation upper bound $\delta \leq \varepsilon + \max(0, g(x) - R)$, not on-chain forced liquidation.

Bright-PCIM peg bound: under VRC-10 currently effective tier parameter C_0 (upper-tier example $C_0 \approx 161.8\%$), no L/W , oracle mint/redeem same-price with arbitrage bandwidth ε , and protocol reserves as share of circulation R , after BTG falls x relative to the reference price, Bitcurrency secondary peg deviation δ 's upper bound is ε (when $x < x^*$) or $\varepsilon + \max(0, g(x) - R)$ (when $x \geq x^*$), where $g(x) = \max(0, 100\% - C_0(1 - x))$. This upper bound can be tested by mainnet data: if mainnet observes δ persistently above the derived value, that indicates arbitrage failure, insufficient reserves, or oracle definitional split—not that the model “automatically holds.”

Three-chain closure (peg must be jointly set by the following three chains, not a single parameter):

Oracle chain: mint and redeem read the same TWAP + redundant median; single-block anomalous deviation triggers circuit breaker—pause new mints, retain additional collateral and redemption.

Collateral chain: C_0 is current-tier collateral ratio (must have $C_0 > 100\%$ for overcollateralization); no liquidation line L or warning line W ; $C(x) = C_0(1 - x)$; x^* is the critical drawdown where coverage breaks 100%.

Arbitrage chain: when $x < x^*$ mint/redeem arbitrage constrains δ within ε ; when $x \geq x^*$ gap $g(x)$ and reserve R determine δ 's upper bound.

The logical relations of the three chains jointly may be summarized as:

flowchart TD

```

O["Oracle chain: mint/redeem same TWAP + circuit breaker"]
C["Collateral chain: C(x)=C0(1-x), no L/W"]
A["Arbitrage chain: mint-and-sell / buy-and-redeem"]
X["BTG falls x%"]

```

$X \rightarrow C$
 $O \rightarrow A$
 $C \rightarrow |x < x^*| A$
 $C \rightarrow |x \geq x^*| G[\text{"Gap } g(x)"]$
 $G \rightarrow R[\text{"Reserve } R \text{ absorbs"}]$
 $A \rightarrow D[\text{"Peg deviation } \delta \leq \varepsilon"]$
 $R \rightarrow D2[\delta \leq \varepsilon + \max(0, g(x) - R)]$

Model Assumptions

For teachability, the following derivation proceeds under a single-period, isomorphic-position frame—all system initial positions minted at C_0 ; after shock no one adds collateral or partially redeems (conservative stress boundary); oracles and redemption channels still operate normally at the shock instant; R is protocol reserves as share of circulating Bitcurrency, injectable into redemption when gaps appear. Multi-issuer games, cross-protocol BTG contention, and governance parameter changes are omitted—these may make actual δ higher than lower bounds without changing comparative-static direction.

Peg closure depends on three chains: oracle pricing $\rightarrow$ overcollateralization constraints $\rightarrow$ mint/redeem arbitrage. VRC-10 does not set liquidation line L or warning line W (distinguishing MakerDAO/CDP); when C breaks 100% it does not trigger on-chain forced auctions; risk becomes redemption runs and reserve consumption—the structural divide from DAI-style CDPs.

Oracle architecture: on-chain DEX Bitgold/stable-asset TWAP (e.g., 1-hour window) as primary feed; multi-node median or trimmed mean as redundant check; if single-block price deviation exceeds threshold θ (e.g., 20%), trigger circuit breaker—pause new mints, allow only additional collateral and redemption, preventing flash-loan feed manipulation. Mint and redeem both read the same oracle, avoiding “high-mint, low-redeem” definitional split.

Arbitrage channels: when secondary price $p > 1 + \varepsilon$, participants stake Bitgold at C_0 to mint Bitcurrency and sell—supply rises, p falls; when $p < 1 - \varepsilon$ and positions are healthy, participants buy Bitcurrency at market and redeem Bitgold—supply contracts, p rises. As long as collateral covers debt and redemption channels are open, δ is theoretically constrained by ε .

Comparative Statics: BTG Falls $x\%$ $\rightarrow$ Deviation Upper Bound

Four-step derivation chain:

Step	Input	Equation / judgment	Output
1 Initial	Debt face D , current tier C_0 (upper-tier example 161.8%)	Collateral MV = $C_0 \cdot D$	Excess issuance
2 Shock	BTG falls $x\%$	$C(x) = C_0(1 - x)$	Coverage falls
3 Gap	$C(x)$ vs 100%	$g(x) = \max(0, 100\% - C(x))$; $x^* = 1 - 100\%/C_0$	Whether hard collateral insufficient
4 Deviation	$g(x)$, R , ε	$x < x^* \Rightarrow \delta \leq \varepsilon$; $x \geq x^* \Rightarrow \delta \leq \varepsilon + \max(0, g(x) - R)$	Peg upper bound

Derivation (Step 2). At mint, debt face is D , collateral MV is $C_0 \cdot D$. After Bitgold falls x relative to the oracle reference ($0 \leq x < 1$), collateral MV becomes $C_0(1 - x) \cdot D$, hence post-shock collateral ratio:

$$C(x) = \frac{C_0(1 - x) \cdot D}{D} = C_0(1 - x)$$

I.e., coverage falls linearly with BTG drawdown—the sole core equation of peg comparative statics.

Proposition 1 (coverage critical drawdown). Under isomorphic positions and no additional collateral, the critical drawdown at which collateral MV no longer covers debt face ($C < 100\%$) is:

$$x^* = 1 - \frac{100\%}{C_0} = 1 - \frac{100\%}{161.8\%} \approx 38.2\%$$

I.e., when Bitgold falls about 38.2% from the reference, isomorphic initial positions' hard on-chain collateral exactly reaches the face-coverage line—no forced liquidation triggers, but redemption and peg pressure rise sharply.

Proposition 2 (peg upper bound in the safe zone). If $x < x^*$ and oracles and redemption channels are normal, arbitrage can operate; secondary-price deviation' s upper bound approximates:

$$\delta \leq \varepsilon$$

Proposition 3 (peg pressure in the undercoverage zone). If $x \geq x^*$, on-chain collateral insufficiently covers debt in full; the gap is:

$$g(x) = \max\left(0, \frac{100\% - C(x)}{100\%}\right)$$

VRC-10 has no automatic liquidation auctions; under the simplifying assumption that reserve R can fully absorb the gap and redemption channels are open, secondary-price deviation' s upper bound approximates:

$$\delta \leq \varepsilon + \max(0, g(x) - R)$$

If $R < g(x)$ or redemption queues are too long, δ may significantly exceed ε —upper bounds need scenario estimation, not promises.

Three propositions jointly—oracle same-price + collateral constraints + arbitrage channels; all three chains indispensable:

$$\underbrace{C(x) = C_0(1 - x)}_{\text{collateral chain}} \wedge \underbrace{\text{mint price} = \text{redeem price} = \text{TWAP}}_{\text{oracle chain}} \Rightarrow \underbrace{\delta \leq \begin{cases} \varepsilon & x < x^* \\ \varepsilon + \max(0, g(x) - R) & x \geq x^* \end{cases}}_{\text{arbitrage chain}}$$

This is PCIM peg' s minimal closed form: given C_0 , x , ε , R , one can compute peg-deviation upper bounds; given observed δ and x , reverse-infer whether reserves are adequate or arbitrage has failed—the model is testable by mainnet data, not merely restatable.

Numerical example (upper tier $C_0 \approx 161.8\%$): at $x = 40\%$, $C(40\%) = 161.8\% \times 0.6 = 97.1\%$, $g(40\%) = 2.9\%$ —if the whole system is isomorphic and no one adds collateral, theoretical collateral gap is 2.9% of debt face; δ is no longer constrained by ε alone. If protocol reserves $R = 3\% \geq g(40\%)$ and redemption channels are open, Proposition 3 gives $\delta \leq \varepsilon + \max(0, 2.9\% - 3\%) = \varepsilon$ —about 0.5% is a stress estimate, not a promise; if $R < g(x)$ or liquidity drying lengthens redemption queues, δ can amplify significantly.

Reverse-inference check (upper-tier example $C_0 \approx 161.8\%$): if on-chain current tier is the upper tier, the oracle reports BTG already down $x = 30\%$ (hence $C(x) = 113.3\%$, $x < x^*$), while secondary $\delta = 3\%$ and $\varepsilon = 0.5\%$, then $\delta \gg \varepsilon$ indicates arbitrage- or oracle-chain anomaly—not collateral-chain insufficiency (here $g(x) = 0$). Conversely, if $x = 45\%$ ($g(45\%) = 8.1\%$), $R = 2\%$, and $\delta = 7\%$, then $\delta \approx \varepsilon + (g - R) = 0.5\% + 6.1\%$ matches the upper bound; pressure mainly from collateral gap not fully absorbed by reserves—monitor redemption queues and R consumption rather than waiting for on-chain forced liquidation.

Comparative-statics quick table (upper-tier example $C_0 \approx 161.8\%$, $R = 3\%$, $\varepsilon = 0.5\%$ scenario assumptions; VRC-11 column for layered contrast only—does not apply Proposition 2’ s $\delta \leq \varepsilon$ upper bound):

BTG drawdown x	$C(x)$ (VRC-10)	$g(x)$ (VRC-10)	δ upper bound (VRC-10)	$C(x)$ (VRC-11)	$g(x)$ (VRC-11)
0%	161.8%	0%	$\leq \varepsilon$	61.8%	38.2% (structural)
20%	129.4%	0%	$\leq \varepsilon$	49.4%	50.6%
38.2% (x^*)	100.0%	0%	$\leq \varepsilon$	38.2%	61.8%
40%	97.1%	2.9%	$\leq \varepsilon$ ($R \geq g$)	37.1%	62.9%
50%	80.9%	19.1%	$\leq \varepsilon + 16.1\%$	30.9%	69.1%

Reading points: 38.2% in the VRC-10 row is x^* (excess buffer exhausted, coverage exactly 100%); in the VRC-11 row it is $g(0)$ (structural gap from the first mint)—same number, two semantics; must not be juxtaposed with “38.2% stake overcollateralization.” When $x \geq x^*$ VRC-10’ s δ upper bound amplifies linearly with $g(x) - R$; VRC-11, because $C_0 < 100\%$, must separately assess peg via whitelist acceptance circles and off-chain redemption—do not apply the last column’ s δ formula.

The model deliberately omits multi-issuer games, cross-protocol BTG contention, and governance parameter changes—from it one can induct several observable implications of PCIM peg mechanisms:

Mechanism implication	Observable metric	If expectations unmet
When $x < x^*$, δ should near ε	Bitcurrency secondary p deviation when BTG daily drawdown $< 38.2\%$	Redemption channels normal yet persistent $\delta \gg \varepsilon$
When $x \geq x^*$, δ amplifies with $g(x) - R$	On-chain $C(x)$, reserve consumption, and p depeg amplitude	Gap expands yet δ does not rise (arbitrage/reserves anomalously effective)
During oracle circuit breaker, upward δ risk rises	Duration of $p > 1 + \varepsilon$ while new mints paused	After breaker p still constrained by ε with no reserve consumption
Governance parameter changes must be monitorable ex ante, not flash-passed	Crisis expansion proposals must trigger split-track quorum + timelock	Crisis single-block passage of cut C_0 or unilateral expansion with no exit window
Reserve transparency and run coordination (Ahmed et al. 2024)	Probability of coordinated holder exit after disclosing reserve composition/volatility	Low-prior disclosure accelerates runs; R volatility not in model

All the above implications can be tested in mainnet or testnet stress data; the model gives upper bounds, not promises—actual δ may exceed derived values due to liquidity drying, cross-protocol contention, or governance parameter changes.

If Oracles Fail or Redemption Crowds: Protocol-Side Responses and Unsolved Boundaries

When oracles are manipulated or sampling too narrow (thin-pool TWAP flash-loan pumped), wrong feeds can cause over-minting or redemption mispricing—historically multiple lending protocols incurred bad debt from feed attacks. PCIM’ s design response: multi-source TWAP + redundant median, single-block anomaly circuit breaker pausing new mints, mint and redeem reading the same definition to avoid “high-mint, low-redeem.” When OTC and DEX depth are insufficient (Ferraro, Kan & Sunderam 2022 “Stable Coins but Thin Markets”), even if reserves and collateral ratios are on-chain verifiable, pegs may still deviate as redemption queues lengthen—Grobys et al. (2021) multi-stablecoin peg-deviation panels agree: fiat-collateralized volatility is usually lower than algorithmic, but all classes can show significant δ under thin markets; Brauneis et al. (2024) further show peg-deviation

amplitude systematically amplifies when OTC/on-chain depth is insufficient—oracle and arbitrage chains must be jointly designed with market depth, not closable by parameter tables alone¹¹. When reserve R 's composition and volatility are incompletely observable to holders (Ahmed, Aldasoro & Duley 2024), publicly disclosing reserve quality may raise run risk under low priors—on-chain readable C_0 and reserve-ratio tables do not eliminate coordination games; PCIM must bring reserve-asset volatility into scenario assumptions for R consumption and Bright-PCIM peg bound, not disclose static ratios alone¹². When circuit breakers have triggered and secondary $p > 1 + \varepsilon$, one-way arbitrage fails and upward δ risk rises—dependence on reserve R and secondary depth, not closable by the model alone.

If Bitgold plunges trigger redemption runs rather than Maker-style forced-liquidation cascades: PCIM sets no liquidation lines; participants concentrate on redeeming Bitcurrency to unlock BTG, possibly jointly depressing BTG prices and consuming protocol reserves—March 2020 MakerDAO “Black Thursday” showed automatic liquidation itself can amplify declines¹³; PCIM deliberately avoids that path, but redemption queues and reserve consumption when liquidity dries may be slower and less predictable than on-chain auction cascades. Open questions remain: thin-pool TWAP can still be attacked; cross-protocol BTG contention synchronously tightens three-layer coverage; whether decentralized oracles and redemption channels suffice under extremes still awaits practice, not white-paper promises.

Terra/UST Contrast: Which Class PCIM Belongs To, and Which Traps to Avoid

The 2022 Terra/UST collapse was failure of algorithmic stablecoin + dual-token self-reinforcing burn-mint, not of overcollateralized CDPs: UST mainly relied on LUNA burn/mint and Anchor high yields to maintain the peg, lacking hard collateral coverage always above 100%; LUNA price falls → mint more LUNA to absorb UST → LUNA falls further—a death spiral¹⁴. Clements (2021) argued before Terra's collapse that algorithmic stablecoins depend on three conditions historically never guaranteed simultaneously—baseline demand, arbitrageur participation, reliable feeds—UST's “confidence-collapse run” triggered by large Curve-pool sells aligns with Adams & Ibert (2022) ex-ante empirics on Iron/Titan algorithmic runs¹². Catalini, Goren & Shah (2021) divide stability mechanisms into fiat-collateralized, crypto-overcollateralized, and algorithmic, noting unsustainable subsidies as a precondition of algorithmic depeg—UST belongs to the third class stacked with Anchor high-yield subsidies, not PCIM's second class¹¹. Liu et al. (2023) on-chain empirics show large, high-information participants exit first in early depeg (sophisticated-first exit); Anchor's ~20% deposit APY accelerated that order when subsidies became unsustainable—dual failure of Tokenomics and stability mechanism, not mere “market panic”¹⁴. Distinguish two “38.2%” types: $\$x^{\wedge} \text{ approx } 38.2\% \$^*$ is VRC-10 overcollateralization's BTG critical drawdown (threshold where coverage breaks 100%), not a stake ratio—VRC-10 upper-tier stake ratio ~161.8%, 61.8% is excess buffer; VRC-11 private-layer 61.8% stake ratio is the undercollateralization parameter—the two must not be conflated.

PCIM's place in the stability-mechanism spectrum: same class as MakerDAO/DAI—overcollateralized CDP—each Bitcurrency unit at issuance has $C_0 > 100\%$ Bitgold locked; essential boundary with UST-style “pure algorithm + undercollateralized expansion”¹⁵. Competitive issuance changes issuer count and rule transparency, not the hard constraint that “collateral MV must cover debt.”

Traps to actively avoid: (1) undercollateralization or self-reinforcing expansion—must not fill collateral gaps with Bitgold inflation or dual-token burn alone; (2) stablecoin native high yields—if Bitcurrency deposit rates persistently exceed real protocol yield and are subsidized by token issuance, that copies Anchor-style Ponzi structures; (3) oracle sampling too narrow—thin-pool TWAP flash-loan manipulable, wrong mint or redeem pricing; (4) crisis governance casually cutting C_0 or unilaterally expanding—parameter transparency $\neq$

parameter credibility; need timelock and multisig constraints; (5) cross-protocol BTG contention—when VRC-10/11/12 expand synchronously, collateral coverage tightens for the whole ecosystem at once.

Transparency $\neq$ stability—UST’ s rules were equally public yet died of design-category error. PCIM’ s theoretical promise is: under overcollateralization + verifiable redemption, use C_0 , x^* , and δ upper bounds to turn “constant value” from slogan into computable constraint; whether extremes deliver still awaits practice, not white-paper self-confirmation.

Common Objections and Mechanism Boundaries

The following table summarizes main objections already developed in the book and protocol-side response points. The book’ s thesis centers on constraint carriers shifting toward verifiable rules; it does not claim full replacement of tax anchors, lenders of last resort, 2% target welfare functions, or MMT macro space.

Objection	Protocol-side points	Still to be tested
Terra/UST death spiral	PCIM is overcollateralized CDP ($C_0 > 100\%$); must avoid Anchor high yields and dual-token gap-filling; Clements (2021) triad; x^* is critical drawdown not stake ratio	Cross-protocol composition may still indirectly import undercollateralized “reserves”
Liquidation cascades and oracle failure	No $L/W \rightarrow$ redemption-run main path; TWAP+breaker+same-price mint/redeem; Ahmed et al. (2024) reserve-disclosure paradox; three-layer BTG contention	Thin-pool manipulation, redemption queues slower than model, cross-venue arbitrage failure, low-belief disclosure accelerating runs
Governance capture	Split-track quorum, timelocks, crisis pause forbidding unilateral expansion	Staged erosion under concentration; on-chain democracy slower than central-bank coordination; Aquilina et al. (2023) issuance concentration
Chartalist / lender of last resort	Tax anchors explain fiat demand, do not automatically imply seigniorage must be monopolized; protocols supply auditable parallel discipline	Crisis fiat and on-chain redemption depth may dry simultaneously
New Keynesian 2% target	Protocol side moves issuance constraints onto verifiable state machines	Cannot replicate countercyclical fiscal–monetary coordination and ELB guidance (Blanchard 2010; Schmitt-Grohé & Uribe 2014)
Fine-grained MMT	Under weak institutions inflation constraints can quickly materialize; protocols supply exit options	Missing institutional guardrails in high-inflation democracies
DeFi collateral thresholds and MEV	VRC-10/11 layered thresholds; MEV observable $\neq$ eliminable	No L1 MEV zeroing guarantee; redemption runs + MEV can stack
“Competing currencies are already happening”	Three-definition tests; institutional transition still early	Advanced retail legal-tender/tax anchors still lock to local currency for the foreseeable future (Ma et al. 2023)

Section 10. Openverse Evolution Path: Layer 0 Value-Exchange Layer and the World Value Network

The white paper describes Openverse’ s realization as a long, uncertain, iterable engineering process and draws three technical–economic steps—isomorphic with gradual-adoption monetary-reform paths. This book’ s core positioning of the architecture must be distinguished from white-paper engineering terms: Openverse is not

a closed hub of “one Hub with several Zone subnets,” but is positioned as Layer 0—a globally decentralized value-exchange layer: at the protocol layer providing value addressing, routing, final-settlement anchoring, and cross-domain interoperability, so that Ethereum, Cosmos ecosystem chains, consortium chains, and Openverse ecosystem app chains and other Layer 1 networks can all access, without custom bridges for every chain pair. White-paper Hub Chain corresponds to the Layer 0 core chain (POS consensus, validator staking and slashing, cross-domain clearing anchors; protocol layer does not host application smart contracts); Zones correspond to ecosystem-native Layer 1 app chains (VMs, contracts, concrete business)—the two are implementation layering atop Layer 0, not Openverse’s full boundary; external Layer 1s accessing Layer 0 via VTP, IBC, and similar standards complete the “world value-exchange network” picture.

Openverse 2.0 (public-currency operating platform) is the current-stage focus: atop Versed (Go-language implementation of the value protocol) and the Layer 0 mainnet, with Bitgold as underlying standard asset, competitively issuing Bitcurrency for each fiat unit via PCIM, and connecting DEXs and payment scenes at the application layer so public currency moves from protocol state into settleable, composable economic activity. The Layer 0 core chain handles consensus security, stake slashing, and cross-domain state anchoring; ecosystem Layer 1 app chains host smart contracts and high-frequency business—separating value exchange and final settlement (Layer 0) from application innovation (Layer 1), lowering coupling between global security paths and local business iteration.

Openverse 3.0 (world value-exchange network) plans to strengthen Layer 0’s cross-domain capacity: introducing homogeneous chain groups so industry alliances and regional ecosystems can run independent Layer 1 instances sharing Layer 0 security; simultaneously extending VTP cross-chain value transfer, Universal Name Service (UNS, mapping long addresses to readable names), and standard suites for metaverse interoperability—positioning ascending from “single-chain hub” to decentralized value-exchange infrastructure that can admit many Layer 1s, not a closed Hub/Zone LAN.

Openverse 4.0 (distributed economic ecosystem) faces heterogeneous Layer 1 clusters and third-party blockchain protocol compatibility, focusing on ecosystem access and cross-chain value routing rather than single-chain performance narratives.

The white paper also lists engineering principles: full decentralization, resilience, security, simplicity (protocol layer does not host application logic), durability (including forward-looking consideration of quantum threats), environmental friendliness (POS energy narrative relative to POW). These principles echo the global ledger infrastructure discussed in Chapter 6; realization degree must be tested by mainnet operating data and external audits, not white-paper self-description.

Section 11. Private-Domain Stability and the Asset-Token Layer

Public currency solves “public pricing and settlement in open networks”—anyone holds, any protocol accepts, on-chain globally visible. Real economic activity largely occurs within permission boundaries: intra-enterprise transfers, supply-chain finance, compliant-network settlement. These scenes need VRC-11 (Privcurrency, private-domain stablecoin) and VRC-12 (Bitsecurity, security-type tokens)—respectively providing within-boundary stable settlement units and tokenization bases for enterprise equity/RWA, forming with VRC-10 a complete spectrum from public to private, from money to securities. Private-layer parameters, compliance, and RWA deployment paths are developed later and in dedicated chapters.

The experimental significance of VRC-10 and PCIM exceeds any single protocol: it represents one class of exploration into whether monetary issuance rules can be on-chained, transparentized, and multi-agent-participated; conclusions must be tested by time and markets. Popularization’s true meaning is that participants

can join in understandable, verifiable ways—not passively hold unauditable assets—but “more people can participate” and “more people can understand what they participate in” are two levels; the latter needs risk explanation, simulation tools, and community learning resources, or else information asymmetry is only more widely dispersed.

Section 12. Comparative Analysis with Traditional Monetary-Policy Transmission

PCIM’s significance must be examined in a comparative frame with traditional monetary-policy transmission. In fiat systems, central banks adjust policy rates, open-market operations (buying or selling Treasuries), reserve-requirement ratios, and other tools to affect commercial banks’ lending costs and thence investment and consumption in the real economy. That transmission chain involves multiple intermediaries (commercial banks, financial markets); effects often have lag and uncertainty. In *The General Theory*, Keynes stressed that when the economy falls into deep recession and rates near the zero lower bound, monetary policy may “push on a string”—central banks can supply liquidity yet cannot force pessimistic firms and households to raise effective demand¹⁶.

PCIM supplies a different transmission path: per white-paper design, collateral-ratio parameter C_0 directly determines how much Bitcurrency each Bitgold unit can issue—a local mirror of statutory reserve ratios; redemption runs and circuit-breaker pauses constitute market-level credit-contraction signals; governance votes perform parameter-revision functions. But the key difference: traditional monetary policy targets economy-wide aggregates measured in billions, jointly with employment, inflation, output, and the ELB—empirics of QE exit and procyclical credit contraction (including SVB’s 2023 failure and AFS duration mismatch). PCIM currently (if landed per white-paper roadmap) serves relatively closed protocol ecosystems; policy-transmission range and depth are not comparable to fiat systems.

This is positioning, not criticism. PCIM per white-paper design supplies protocol-ecosystem participants a transparent, participable, discipline-constrained monetary frame—within its as-yet-unverified limited range, a debatable participation-structure experiment; whether it can transmit outward as the ecosystem scales depends on compliance interfaces and OTC depth—a gradual evolutionary path, not overnight institutional replacement.

Section 13. Information-Theoretic Foundations of Monetary Popularization

Reexamining PCIM and monetary popularization from an information-theoretic angle yields a new analytical dimension. One of Hayek’s core insights is the price system as a coordination mechanism for dispersed knowledge: no central planning agency can master society’s dispersed, local, personalized knowledge, yet the price system, by aggregating countless individual decisions, spontaneously integrates that knowledge. Money as the price system’s foundation—its quality directly affects knowledge-integration efficiency. Keynes in *The General Theory* pointed from another path: expectations and confidence themselves are critical aggregate-demand variables—even with public information, if participants are broadly pessimistic about the future, price signals can scarcely activate investment¹⁷.

On-chain protocols supply a novel public-knowledge production mechanism at the information layer. Every on-chain transaction, every stake and redemption, every governance proposal and vote becomes publicly inspectable “protocol-state knowledge” any participant can obtain in real time. Versus fiat systems’ periodic release of central-bank minutes and quarterly commercial-bank balance sheets, frequency is higher, accessibility stronger, and without institutional information screening and packaging.

This information democratization brings not only transparency improvement but change in knowledge-distribution patterns. In traditional finance, professional investors earn excess returns from information advantage—both stronger acquisition channels and stronger processing capacity. On-chain information’s

publicity weakens the former (acquisition-channel advantage) but cannot weaken the latter (ability to understand and use information). Therefore the real beneficiaries of on-chain information democratization are professional analysts who can process on-chain information, not ordinary participants with limited processing capacity—unless information interfaces and analysis tools’ usability rise in parallel so ordinary people can effectively use public information. That is monetary popularization’ s core challenge on the information dimension.

Further distinguish verifiability from information equality: on-chain collateral ratio C_0 , reserves R , and redemption-queue length can be read by third parties—this is the operational meaning at the PCIM layer of constraint carriers shifting from reputation to verifiable rules—but verifiable $\neq$ understandable $\neq$ actionable. Aramonte et al. (2021) BIS analysis shows DeFi participants’ information-processing capacity regarding oracle definitions, governance proposals, and MEV timing remains highly differentiated⁴; Ma et al. (2023) also show that even with peg state public on-chain, edge-corridor users under stress may still be unable to redeem at quoted prices for lack of OTC depth¹. Fully readable on-chain state does not mean ordinary people already master monetary information—reading Bright-PCIM peg bound, distinguishing VRC-10/11’ s two 38.2% semantics, assessing whether cross-venue arbitrage has failed remain professional thresholds for most retail participants. Whether information interfaces and analysis tools’ usability can keep pace with expanding state readability will decide whether “popularization” expands participation or expands professional analysts’ relative advantage; the gap between on-chain-readable state and ordinary people making prudent decisions on that basis is no smaller than the gap between “dusk” and “midnight” in early institutional transition.

Section 14. Public Currency’ s Historical Coordinates

In the long river of monetary history, PCIM and Bitcurrency’ s place is quite distinctive. Across monetary history, every major evolution of monetary form accompanied transfers of issuance rights and rewriting of issuance rules: from barter to metallic coinage (issuance rights from dispersed individuals to rulers); from metallic money to paper (from coinage sovereignty toward commercial-bank credit expansion); from gold standard to fiat (from physical anchors to state-credit backing); from fiat to digital money (from physical presence to digital representation).

Every evolution had institutional premises: rulers’ authority securing coinage credit; commercial-bank regulatory frames securing paper credit; central-bank independence securing fiat credit. PCIM tries to replace these traditional credit bases with protocol code and decentralized governance—a new experiment not yet fully verified by historical precedent. On these historical coordinates, Openverse’ s attempt is the newest link in humanity’ s long monetary-evolution chain; its significance must be evaluated in the whole historical sequence, not only compared with Bitcoin or Ethereum.

注释与引用

1. DeFi Llama Stablecoins Dashboard (2024): peak total market cap of USDT/USDC etc. ~\$180 billion order; Artemis Analytics estimates 2024 global stablecoin on-chain nominal volume ~\$33 trillion (cited by Bloomberg etc.); Visa Onchain Analytics Dashboard (2025) “adjusted” 12-month volume ~\$10.2 trillion; McKinsey & Artemis, *Stablecoins in payments: What the raw transaction numbers miss* (2025): real payment flows ~\$390 billion/year, ~0.02% of global payments; Ma, Ganesh, Andreas Schrimpf, and Andreas V. I. Pereira (2023), IMF WP 23/72 “Stablecoins amid Crypto Winter”: stress-period stablecoin flows synchronized with crypto-market liquidity. Three-definition gaps and “possibility $\neq$ reality” discipline in Chapter 1, Section 8.

↩ ↩² ↩³ ↩⁴

2. Schumpeter, 1954, *History of Economic Analysis*, chapters on money and banking history: tracing monetary forms from commodity to credit, from private notes to central banks. Oxford University Press 1954 edition. ↵
3. Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. "An empirical study of DeFi liquidations." *IMC* 2021, pp. 336–350: MakerDAO etc. longitudinal liquidation data, Black Thursday auction mechanisms; Eisenberg & Schär (2021), "DeFi Liquidations," *AFT* 2021. <https://arxiv.org/abs/2106.06389> ↵
4. Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf. "DeFi risks and the decentralisation illusion." *BIS Quarterly Review*, December 2021, pp. 21–36: oracle, governance, and liquidity concentration; Chitra & Angeris (2020), "Improved Price Oracles: Constant Function Market Makers," *AFT* 2020: TWAP jointly designed with pool depth; Aspris (2024), SSRN WP 4913633: Maker vault-level leverage and forced liquidation; S&P Global (2023); Chitra et al. (2024), *Frontiers in Blockchain* 7, 1392812 (DAISIM). https://www.bis.org/publ/qtrpdf/r_qt2112e.htm ↵ ↵²
5. Barbon, Andrea, and Angelo Rinaldo (2024), "On the Quality of Cryptocurrency Markets: Centralized versus Decentralized Exchanges," *Management Science* forthcoming; arXiv:2112.07386: under CEX/DEX segmentation, arbitrage chains and δ upper bounds need scenario correction. <https://arxiv.org/abs/2112.07386> ↵
6. Brunnermeier & Niepelt (2020), "On the Equivalence of Private and Public Money," *Journal of Monetary Economics* 106, pp. 27–41; Bindseil (2024), ECB OP 322, §§5–6 (payment-type vs investment-type CBDC, holding caps); Auer, Cornelli & Frost (2022), "CBDC and financial stability," *BIS Quarterly Review*, March 2022, pp. 55–68. <https://doi.org/10.1016/j.jmoneco.2019.10.006> ↵
7. Lyons, Richard K., and Ganesh Viswanath-Natraj. "What Keeps Stablecoins Stable?" NBER Working Paper 27136, May 2020 (revised 2022): reserve redeemability and OTC depth; Griffin, John M., and Amin Shams. "Is Bitcoin Really Untethered?" *Journal of Finance* 75(4), August 2020, pp. 1913–1964: fiat-collateral reserve transparency controversies; Viswanath-Natraj & Lyons (2023), *Journal of International Money and Finance* 131, 102777: USDC stress-period pricing dynamics. <https://www.nber.org/papers/w27136> ; <https://doi.org/10.1111/jofi.12815> ↵ ↵²
8. Rockoff, Hugh, "The Free Banking Era: A Reexamination," *JMBC* 6(2), 1974, pp. 141–167; Rockoff, "Lessons from the American Experience with Free Banking," in Dowd (ed.) (1992), ch. 4, pp. 73–86; Kroszner, Randall S., "Free Banking: The Scottish Experience as a Model for Emerging Economies?" *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31 (Scottish experience not directly extrapolable to anonymous global on-chain parallelism). ↵
9. Szabo (2005), "Bit gold"; Szabo (1997), "The God Protocol" (verifiable third-party substitute); Szabo (1999), "Trusted Third Parties Are Security Holes"; Szabo (1998), "Secure Property Titles with Owner Authority"; Szabo (2002), "Shelling Out: The Origins of Money" (collectibles cooperation → monetary cooperation); Finney (2004), "Reusable Proofs of Work (RPOW)"; Nakamoto (2008), §§1–2 (timestamp server, longest chain); Back (2002), Hashcash §§1–3 (PoW precursor). Openverse Foundation, *Bitgold Whitepaper* v2.1.5 (source: official white paper v2.1.5, not independently audited). <https://nakamotoinstitute.org/the-god-protocol/> ; <https://nakamotoinstitute.org/shelling-out/> ; <https://nakamotoinstitute.org/trusted-third-parties/> ; <https://nakamotoinstitute.org/library/finney-rpow/> ; <https://bitcoin.org/bitcoin.pdf> ↵ ↵²
10. Szabo (2017), "Money, Blockchains, and Social Scalability": social scalability—verifiable rules replacing interpersonal trust costs. <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↵
11. Ferraro, Gianni, Kan Li, and Adi Sunderam. "Stable Coins but Thin Markets." Princeton Economics Working Paper No. 1416, October 2022 (revised 2023): pegs more fragile when OTC depth insufficient; must jointly design with oracle and arbitrage chains; Grobys, Klaus, Juha Juntila, James W. Kolari, and Niranjana Sapkota. "On the stability of stablecoins." *Journal of Empirical Finance* 64(C), 2021, pp. 207–223: multi-stablecoin peg-deviation panels, mechanism type and volatility; Brauneis, Alexander, et al. "How stable are stablecoins?" *European Journal of Finance* 30(9), 2024, pp. 1027–1058: peg-deviation amplification under thin markets; Catalini, Christian, Alon Goren, and Divya Shah. "Some Simple Economics of Stablecoins." MIT Sloan Research Paper, November 2021 (revised 2022): fiat-collateralized / crypto-overcollateralized / algorithmic trichotomy and unsustainable-subsidy conditions. <https://www.princeton.edu/~kan/StableCoins.pdf> ; <https://doi.org/10.1016/j.jempfin.2021.09.002> ; <https://doi.org/10.1080/1351847X.2023.2240254> ; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968382 ↵ ↵²
12. Clements, Ryan (2021), "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins," *Wake Forest Law Review Online* 11, 131–171 (algorithmic triad: demand, arbitrage, feeds); Adams, Austin, and Markus Ibert (2022), "Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel," *FEDS Notes*, June 2, 2022 (ex-ante empirics of algorithmic runs); Ahmed, Rashad, Iñaki Aldasoro, and Chantelle Duley (2024/2025 rev.), "Public information and stablecoin runs," BIS Working Paper

- 1164 (reserve-quality disclosure and run-coordination paradox; P5 testable proposition). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3952045 ; <https://doi.org/10.17016/2380-7172.3121> ; <https://www.bis.org/publ/work1164.htm> ↩ ↩²
13. MakerDAO Risk Team (2020-03-12), “Black Thursday Post Mortem”: ETH crash triggering liquidation spirals and zero-price auctions; Liu et al. (2023) NBER WP 31160 and HKMA RM09-2022 contrasting UST redemption runs with CDP liquidation-cascade contagion paths. Forum: <https://forum.makerdao.com/t/black-thursday-post-mortem/1853> ↩
14. Brunnermeier, Niehaus & Schab (2022), BIS Bulletin No. 63; Terra Form Labs (2019, source: official white paper v1, not independently audited): dual-token burn/mint mechanisms; IMF (2022), *GFSR* October issue Ch. 2, pp. 43–78; Liu, Makarov & Schoar (2023), NBER WP 31160: Terra on-chain sophisticated-first exit and Anchor high-yield subsidy exit order. ↩ ↩²
15. Schär (2021), *FRB St. Louis Review* 103(2), pp. 153–174: MakerDAO Purple Paper CDP and liquidation-line design; Lyons & Viswanath-Natraj (2020), NBER WP 27136: empirical framework for reserve redeemability and peg stability; Klages-Mundt et al. (2023), *Journal of Financial Stability* 68: stablecoin mechanism spectrum taxonomy. ↩
16. Keynes, 1936, *The General Theory of Employment, Interest and Money*, Chs. 15 and 21: monetary-policy limits under liquidity traps, and reliance on fiscal policy and confidence restoration when effective demand is insufficient. Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩
17. Keynes, 1936, *The General Theory of Employment, Interest and Money*, Ch. 12: expectations and “animal spirits” as central to investment and aggregate demand—“Our estimate of the probability of success ... ultimately rests on an act of intuitive judgment.” Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩

§ 15 Private-Domain Stability and On-Chain Assets

Public currency solves open-network pricing and settlement; much economic activity, however, occurs in private domains with boundaries, permissions, and compliance constraints. VRC-11 (Privcurrency, private-domain stablecoin) is a stable-settlement scheme customized for particular groups, scenes, or organizations—not public currency for undifferentiated audiences. Openverse’s *VRC-11 Blue Paper* (v2.0.0) positions it as an “enterprise-/nation-grade private-domain stablecoin protocol.” This chapter discusses layered design, 61.8% undercollateralized minting, protocol functions and VRC interchange, structural differences from USDT, Bitgold linkage theory, enterprise applications and compliance frameworks, and VRC-12 security-type tokens and risk structure.

Section 1. Why a Private-Domain Layer: The Economic Logic of Protocol Stratification

Public currency cannot cover every scene; its openness has boundaries that must be seen clearly first.

Public currency’s hallmark is openness: anyone may participate, any node may hold, on-chain data are globally visible. That is its strength and its limit. Inter-enterprise settlement, supply-chain finance, and industrial-park internal incentives often have clear participant boundaries—banks will not lend to anonymous addresses; institutional investors will not disclose holdings globally; compliance departments cannot accept payments without KYC.

Traditional economies exhibit the same layering: central banks issue M0 (public domain); commercial-bank deposits are M1/M2 in permissioned systems (private domain); commercial paper and trade credit are narrower private-domain instruments. Each layer has different acceptance circles, issuance rules, and regulatory frames. Openverse’s VRC protocol spectrum is, in a sense, an on-chain version of this logic: VRC-10 corresponds to public base money; VRC-11 to private-domain stable settlement within permissioned domains; VRC-12 to further equity-type token issuance.

Layered design’s benefit is not only covering more scenes but avoiding design arrogance—trying to solve all monetary and financing needs with a single token type. History shows that designs attempting to unify public settlement, private financing, equity proof, and more with one monetary tool often fail because they cannot optimize all dimensions at once. Diversifying protocol types lets each tool optimize for its service scene and combine on the basis of protocol interoperability.

Section 2. VRC-11: Privcurrency’s Positioning and Scenes

The blue paper defines Privcurrency as a private-domain monetary scheme for specific economic agents: issuance, circulation, and use rules customized to enterprise business logic or closed-ecosystem needs—contrasted with VRC-10 public currency’s “undifferentiated openness.” In *The Denationalization of Money*, Hayek advocated multi-agent issuance and market weeding-out of inferior money; VRC-11 spiritually inherits “competition and choice,” but the path is enterprise private-domain minting under protocol standards—not free private-bank note issue as envisioned in 1976.

Core positioning: a stable settlement unit circulating within clear boundaries and participant lists, reducing exchange-rate noise that interferes with contract performance; minted by staking Bitgold (BTG), not by relying on a single centralized institution’s fiat-reserve promise.

Which scenes need such a tool?

Supply-chain settlement is the most direct. Cross-border procurement chains involve raw-material suppliers, intermediate processors, brand owners, and logistics across multiple stages; settlement usually involves multiple fiat currencies, and exchange-rate swings over full account periods (60–90 days) can consume a sizable share of margins. If stages settle on a shared private-domain stablecoin, FX risk is isolated to entry conversion rather than dispersed across every intermediate settlement. The blue paper uses auto supply chains as example: parts suppliers face two-month production cycles and receivable cycles up to four months, severely tying up cash; core automakers can use Privcurrency to provide stablecoin advance financing to suppliers, with repayment conditions written into smart contracts—the same structural class as Foxconn-style account-period problems in Chapter 18. Institutional adoption must be distinguished: programmable advances describe interface-layer possibility; whether suppliers will price in private-domain units and whether core firms accept on-chain payable transparency must be tested by whitelist expansion speed and off-chain redemption failure rates—cannot infer penetration from contract-deployment counts alone. Even when public stablecoin on-chain nominal flows are large, real goods payments remain marginal (see Chapter 1, Section 8); private-domain tools are narrower still—if any link (KYC, FX, tax) remains open, the scheme stays laboratory-bound.

Park economies and closed ecosystems are another typical scene. Development zones, bonded zones, and industrial parks often want internal points or token systems that incentivize in-ecosystem procurement and consumption while limiting capital outflow and preserving park liquidity-pool scale. If VRC-11 can serve this need within a compliance frame, it is an on-chain upgrade of traditional points systems: programmable, interoperable, with issuance and circulation records inspectable on-chain.

Cross-border trade circles represent an intermediate state: participants are clear (partners with long-term trade relations), but legal systems span multiple jurisdictions; bank-wire arrival times and fees create real friction in high-frequency small-ticket trade. The blue paper cites cross-border trade enterprise scenes: traditional wires may cost 2–3% of transaction value with 3–5 business-day arrival, and FX swings may also erode profits—Privcurrency claims fees can be compressed to the 0.1–0.3% order with near-real-time settlement; these figures are design expectations, to be jointly accounted with actual launch data and compliance costs, not treated as already realized facts. Total cost (FX, compliance, off-ramps, failure retries) must be compared corridor by corridor—pending mainnet and audit data.

Enterprise naming conventions: the blue paper suggests enterprise-issued Privcurrency use “brand prefix + base-currency identifier,” e.g., StarUSD, MicroUSD—the prefix reflecting enterprise or scene (Star for brand, Micro hinting micro-customer service), the USD suffix borrowing the dollar’s global pricing recognition to convey “stable value scale” semantics, without claiming hard dollar peg. Under VRC-11 support, the token is minted by the enterprise staking Bitgold under 61.8% undercollateralization rules; value support comes from partial on-chain collateral plus enterprise reputation and off-chain redemption commitments, not bank reserves or VRC-10-style hard overcoverage. Between naming convenience and legal characterization (unregistered payment instrument or security?) regulatory interpretive space remains.

Relative to VRC-10 public currency, this creates depth: the former emphasizes scene closure and compliance collaboration; the latter open participation and ISO fiat-unit mapping. That depth avoids the naiveté of “one token conquers all” and corresponds to real monetary-layer division of labor—except on-chain division is encoded by protocol type, not only by institutional licenses.

Section 3. VRC-11 Protocol Core: 61.8% Undercollateralized Mint and Redeem

Chapter 14, Section 9 gives the minimal proof model for VRC-10/PCIM public peg (C_0 at the current tier, no L/W , three-chain closure); this section first states VRC-11 private-domain mint rules, then completes the layered

comparison of public/private collateral–liquidation–peg in Section 4.

The blue paper reduces VRC-11’ s theoretical resources to two lines: blockchain decentralized ledgers, and stablecoin value-stability theory; it explicitly cites Hayek’ s competitive issuance and currency choice in *The Denationalization of Money* as background for private multi-currency coexistence—aligned with Part II of this book, yet VRC-11’ s path is an enterprise-grade protocol standard, not free private-bank note issue in the 1976 sense.

Mint rules are VRC-11’ s most distinctive technical parameter: users hold Bitgold (BTG), initiate mint requests through VRC-11-compatible interfaces, and smart contracts compute required stake from on-chain real-time prices—the blue paper requires staking roughly 61.8 of Bitgold value to mint 100 of stablecoin face value, i.e., collateral ratio 61.8%. Emphasize: this is undercollateralization—collateral value from issuance onward is below stablecoin face value—forming a golden-ratio contrast with VRC-10 public currency’ s dynamic-tier overcollateralization (upper tier near 161.8%; see Chapter 14, Section 2.2) ($\varphi \approx 1.618$ and $\varphi^{-1} \approx 0.618$). Private-domain stability therefore cannot close the peg on hard on-chain collateral alone; it must layer enterprise reputation, permissioned whitelist constraints, off-chain redemption commitments, and emergency reserves—61.8% should be read as a protocol risk parameter and scene trade-off, not a long-market-tested optimal ratio. MakerDAO and other DeFi protocols historically adjusted collateral ratios through governance many times—after Black Thursday (2020-03-12) ETH minimum collateral ratios were raised; the 2023 Endgame plan further restructured SubDAOs and MKR governance (source: official Litepaper v1, not independently audited)¹—showing a single constant cannot fit all markets.

Minting is designed to be fully automatic: after verifying adequate stake, the contract credits Privcurrency to the user address; on redemption, users burn or return stablecoins and the contract unlocks Bitgold back to wallets under preset rules. Distributed ledgers record every mint and redeem, aiming to reduce dependence on a single issuer’ s reserve statements—contrasting with USDT-class centralized stablecoins. Strict distinction from VRC-10: 61.8% is undercollateralization (insufficient to cover face value), not public-layer dynamic-tier overcollateralization (upper tier near 161.8%); semantic comparison of the two “38.2%” meanings appears in Section 4.

Value anchoring and adjustment in the blue/white papers is described as: Bitgold within the Openverse ecosystem as underlying value support; when private-domain stablecoin secondary prices deviate from target, encouraging or discouraging mint/redeem changes supply. Mechanism logic resembles Bitcurrency under PCIM, but VRC-11 faces enterprise-custom Privcurrency instances (e.g., an automaker’ s private USD unit); the anchor target is defined by the issuance scene, not a unified ISO fiat code table. Where the blue paper says the stablecoin is “tightly anchored to Bitcoin,” context indicates Bitgold (BTG) rather than BTC; this book uniformly says Bitgold to avoid reader confusion.

To handle concentrated redemption, protocol design includes an emergency-reserve idea: even in extreme markets, user Bitgold unlock demand must still be met to keep redemption credibility—specific reserve scale and triggers must follow on-chain contracts and official technical docs.

Relation to general stablecoin models: besides the Bitgold collateral path, enterprise practice may still use fiat-reserve private-domain tokens (bank-custodied equal fiat). The blue paper focuses on the former; real deployments may be hybrid—core trade circles settle in Privcurrency; external fiat channels use traditional banks. Assessing any instance must first ask: is value hung on Bitgold price volatility, fiat-reserve audit, or both? Whether 61.8% undercollateralization can maintain peg within a permissioned domain has no VRC-10-style δ upper bound to apply—test with instance off-chain redemption records, whitelist acceptance circles, and

secondary δ panels; blue-paper adjustment mechanisms (encourage/discourage mint-redeem) are set as white-paper design and still await mainnet and independent audit—robustness must not be inferred from parameter symmetry (golden-ratio rhetoric) alone.

The blue paper runs VRC-11 atop Openverse Layer 0 distributed value-exchange layer: mint, redeem, and transfer execute automatically by smart contract without a single custodian issuing liability certificates—unlike traditional enterprise “points + bank reserve” dual tracks; the technical trust anchor is protocol and collateral state, not institutional annual reports. Layer 0 provides final settlement and cross-domain routing; enterprise private-domain apps may deploy on Layer 1 chains accessing Layer 0, but VRC-11 collateral and redemption state must be readable and verifiable on Layer 0.

Section 4. Layered Comparison: PCIM Public Peg Closure and VRC-11 Private-Domain Collateral

Chapter 14, Section 9 gives PCIM (VRC-10 Bitcurrency)’s minimal peg model and Bright-PCIM peg bound; building on that model, this section gives layered comparison and joint equations for VRC-11 private-domain minting, completing a closed statement of the three mechanisms—collateral ratio, liquidation, peg—so public and private vocabularies are not conflated.

Mechanism-parameter closure at a glance (VRC-10 / VRC-11):

Parameter	VRC-10 / PCIM	VRC-11 Privcurrency
Collateral ratio C_0	Dynamic tiers (upper tier ~161.8%)	61.8% (undercollateralized, fixed)
Liquidation line L / warning line W	Not set	Not set
Oracle	TWAP + redundant median + circuit breaker θ	Same (mint/redeem same price)
38.2% semantics	x^* : BTG critical drawdown	$g(0)$: structural gap
Peg upper bound	$\delta \leq \epsilon$ or $\delta \leq \epsilon + \max(0, g(x) - R)$	Do not apply VRC-10 bound; whitelist + off-chain redemption

Liquidation-mechanism closure (VRC-10 / VRC-11):

Mechanism	MakerDAO/DAI	VRC-10 / PCIM	VRC-11 Privcurrency
Collateral ratio C_0	Asset-dependent (e.g., ETH 150%)	Dynamic tiers (upper tier ~161.8%)	61.8% (undercollateralized)
Liquidation line L / warning line W	Set; $C < L$ triggers auction	Not set	Not set
When coverage insufficient	On-chain forced auction $\rightarrow$ cascade risk	Redemption run + reserve R absorbs	Off-chain redemption run + emergency reserves
Peg upper bound	Separate accounting via L , auction discount	$\delta \leq \epsilon$ or $\delta \leq \epsilon + \max(0, g(x) - R)$	Do not apply VRC-10 bound; whitelist + off-chain credit

VRC-12 (Bitsecurity) retains independent CDP liquidation thresholds—securities-layer risk is accounted separately; do not conflate with the table above.

38.2% terminology closure: strictly distinguish two parameters—VRC-10 / PCIM collateral ratio C_0 is set by circulation-tier public votes (upper tier ~161.8%; when $\sigma = 61.8\%$ excess buffer ~61.8%); 38.2% appears at the upper tier as critical drawdown $x^* = 1 - 100\%/C_0$, meaning isomorphic positions’ coverage falls below 100%

when BTG drops $\sim 38.2\%$ from the reference price—not “stake 38.2% to mint face 100.” VRC-11 collateral ratio $C_0 = 61.8\%$ (undercollateralized, fixed); 38.2% appears only as structural gap $g(0) = 100\% - C_0$ —from the first mint moment hard on-chain collateral is already 38.2 percentage points short of face value—not a gap that appears only after BTG falls 38.2% . Calling VRC-10 “ 38.2% stake overcollateralization” is mathematically false; conflating VRC-11’s structural gap with VRC-10’s critical drawdown misreads peg-closure conditions.

Collateral-parameter comparison:

Layer	Standard	C_0	L/W	38.2% semantics	Peg-closure path
Public	VRC-10 / PCIM	Dynamic tiers (upper $\approx 161.8\%$)	Not set	Upper-tier $x^* \approx 38.2\%$: BTG critical drawdown	Three-chain closure (oracle + overcollateralization + arbitrage)
Private	VRC-11	61.8% (undercollateralized)	Not set	$g(0) = 38.2\%$: structural gap	Undercollateralization + whitelist + off-chain redemption
Securities	VRC-12	Independent parameters	May set	Separate	CDP-style liquidation + legal title

Public Peg Three-Chain Closure (VRC-10)

PCIM’s peg must be jointly determined by three chains, not a single parameter:

Oracle chain: on-chain DEX Bitgold/stable-asset TWAP (e.g., 1-hour window) as primary feed; multi-node median or trimmed mean as redundant check; single-block price deviation above threshold (e.g., 20%) triggers circuit breaker—pause new mints, allow only additional collateral and redemption; mint and redeem at the same price, preventing “high-mint, low-redeem” split definitions.

Collateral chain: at issuance take currently effective tier $C_0 > 100\%$ (upper-tier example 161.8%); after BTG falls $x\%$, $C(x) = C_0(1 - x)$; $x^* = 1 - 100\%/C_0$ (upper tier $\sim 38.2\%$) is the critical drawdown where coverage breaks 100% . No L/W ; when $C < 100\%$ no on-chain forced auction.

Arbitrage chain: when $x < x^*$, $p > 1 + \varepsilon$ incentivizes mint-and-sell, $p < 1 - \varepsilon$ incentivizes buy-and-redeem, $\delta \leq \varepsilon$; when $x \geq x^*$, gap $g(x) = \max(0, 100\% - C(x))$, $\delta \leq \varepsilon + \max(0, g(x) - R)$ (when reserve R can absorb), otherwise enter redemption-run scenarios.

Liquidation-line contrast: MakerDAO/DAI force-auctions collateral when $C < L$, possibly triggering liquidation cascades; VRC-10 deliberately avoids that path, substituting redemption arbitrage + reserves + circuit breakers—the trade-off is redemption-run risk replacing auction-cascade risk, not eliminating extreme-market pressure. The “mechanism-parameter closure” and “collateral-parameter comparison” tables above already give C_0 , L/W , and buffer semantics.

At the public-layer upper tier, “ 161.8% overcollateralization” means: when mint yield $\sigma = 61.8\%$, minting face 100 Bitcurrency requires staking ~ 161.8 Bitgold—collateral covers and exceeds issuance; low-circulation tiers are higher and more conservative (Chapter 14, Section 2.2). “ 61.8% undercollateralization” is the opposite: minting face 100 Privcurrency requires only 61.8 Bitgold value—hard on-chain collateral alone cannot close the peg; private-domain stability depends more on enterprise reputation, whitelist constraints, and off-chain redemption.

Risk-path contrast (public vs private; neither is MakerDAO-style L/W): VRC-10 relies on $C_0 > 100\%$, mint/redeem arbitrage, oracle circuit breakers, protocol reserves, and issuance caps; position collateral ratio C is for monitoring only and does not trigger on-chain forced auctions. VRC-11 relies on permissioned whitelists, off-chain redemption commitments, emergency reserves, and mint/redeem supply adjustment; C likewise has no liquidation/warning thresholds. Mint and redeem read the same oracle (on-chain TWAP + redundant median + anomaly circuit breaker), preventing VRC-10/11 definitional split.

Peg-maintenance path (public VRC-10): (1) $C_0 > 100\%$ guarantees hard excess at issuance; (2) when $x < x^*$, mint/redeem arbitrage constrains p to $[1 - \varepsilon, 1 + \varepsilon]$, $\delta \leq \varepsilon$; (3) when $x \geq x^*$, $g(x) = \max(0, 100\% - C(x))$, $\delta \leq \varepsilon + \max(0, g(x) - R)$ is a simplified upper bound, not forced liquidation. Private VRC-11, because $C_0 = 61.8\% < 100\%$, has structural gap $g(0) = 100\% - C_0 = 38.2\%$ from the first mint—the gap comes from hard on-chain collateral being short of face by 38.2 percentage points from the start, not from BTG first needing to fall 38.2%; peg depends more on enforceability of redemption commitments, acceptance circles within permissioned networks, and off-chain credit; secondary liquidity is usually weaker than VRC-10, so ε is often larger. Viswanath-Natraj & Lyons (2023) dynamic analysis of USDC shows fiat-reserve stablecoins can also sustain discounts under stress²—Grobys et al. (2021) and Brauneis et al. (2024) peg-deviation panels further show that all mechanism types may systematically amplify δ when OTC/on-chain depth is thin; VRC-11 “dual-track depeg” when off-chain redemption fails must enter the same analytical frame².

Peg joint equations (VRC-10 joint upper bound)—one-to-one with Chapter 14, Section 9, Propositions 1–3:

Chain	Constraint equation	Role
Oracle	Mint price = redeem price = TWAP(BTG); $ \Delta p_{\text{block}} > \theta \Rightarrow$ pause new mints	Same price + anti-manipulation
Collateral	$C(x) = C_0(1 - x)$; $x^* = 1 - 100\%/C_0$; no L/W	Excess buffer + no auction cascade
Arbitrage	$x < x^* \Rightarrow \delta \leq \varepsilon$; $x \geq x^* \Rightarrow \delta \leq \varepsilon + \max(0, g(x) - R)$	Peg-deviation upper bound

The three chains must jointly close the peg: $C_0 > 100\%$ alone cannot automatically guarantee $\delta \leq \varepsilon$ —when oracle definitions split or arbitrage channels jam, depeg can occur even if $x < x^*$; arbitrage alone cannot fill collateral gaps when $x \geq x^*$ —reserve R or additional collateral by participants is required. Only joint operation of the three mechanism chains yields an upper-bound function for peg deviation δ .

Joint upper-bound equations:

$$\begin{aligned}
 C(x) &= C_0(1 - x), & x^* &= 1 - \frac{100\%}{C_0} \\
 g(x) &= \max(0, 100\% - C(x)) \\
 \delta &\leq \begin{cases} \varepsilon & x < x^* \\ \varepsilon + \max(0, g(x) - R) & x \geq x^* \end{cases}
 \end{aligned}$$

Given upper-tier example $C_0 \approx 161.8\%$, x , ε , R , the formula directly computes the peg-deviation upper bound; given observed δ and x , one can reverse-infer whether reserves are adequate or arbitrage has failed—the model is testable by mainnet data, not merely restatable.

Numerical check: let $x = 30\%$, $\varepsilon = 0.5\%$, $R = 3\%$. Then $C(30\%) = 113.3\%$, $x < x^*$, $g = 0$, upper bound $\delta \leq 0.5\%$ —if observed $\delta = 3\%$, pressure is on the arbitrage or oracle chain, not the collateral chain. Let $x = 45\%$; then $C(45\%) = 89.0\%$, $g(45\%) = 11.0\%$, upper bound $\delta \leq 0.5\% + 8.0\% = 8.5\%$ —when the gap is not fully absorbed by R , monitor redemption queues and reserve consumption.

Private VRC-11 comparative statics (same frame, different parameters): because $C_0 = 61.8\% < 100\%$, structural gap $g(0) = 100\% - C_0 = 38.2\%$ exists from the first mint; after BTG falls a further $x\%$, $C(x) = 61.8\%(1 - x)$, gap expands to $g(x) = 100\% - C(x)$. E.g., at $x = 20\%$, $C(20\%) = 49.4\%$, $g(20\%) = 50.6\%$ —hard on-chain collateral is already under half of face value; peg depends entirely on whitelist acceptance circles and off-chain redemption—cannot apply VRC-10’s $\delta \leq \varepsilon$ upper bound. Private and public share $C(x)$, $g(x)$ equations; the difference is only whether C_0 exceeds 100%—the mathematical core of unified public/private collateral terminology.

Oracle architecture: VRC-10 and VRC-11 mint/redeem both read the same TWAP feed + redundant median check; when single-block price deviation exceeds θ , circuit-break—pause new mints, retain additional collateral and redemption. Architecture points: (1) same price: mint price = redeem price = TWAP(BTG), forbidding “high-mint, low-redeem”; (2) same definition: public and private must not use split oracles, or cross-layer arbitrage depeg follows; (3) one-way circuit breaker: anomalies only forbid expansion, not contraction—contrasting Maker-style $C < L$ forced auctions. The oracle chain alone cannot close the peg; it must join $C_0 > 100\%$ (public) or off-chain redemption (private) and arbitrage channels.

Peg-closure summary (one sentence): VRC-10 closes the peg with current-tier overcollateralization (upper tier $\sim 161.8\%$) + oracle same-price + mint/redeem arbitrage; upper-tier $x^* \approx 38.2\%$ is BTG critical drawdown (not a stake ratio); VRC-11 closes the peg with 61.8% undercollateralization + whitelist and off-chain redemption; $g(0) = 38.2\%$ is a structural collateral gap (not a shock threshold). Neither sets L/W .

Boundary with Terra/UST: VRC-10 is an overcollateralized CDP (hard-collateral dimension akin to DAI), not a UST-style algorithmic stablecoin, and does not set DAI-style liquidation lines³. VRC-11 is undercollateralized on-chain, closer to a “on-chain credit + partial collateral” private-domain tool; it must be distinguished from UST-style uncollateralized algorithmic stablecoins and must not be conflated with VRC-10 overcollateralization. Extra private-layer risk: enterprise instances may layer off-chain credit promises (“StarUSD redeemable for fiat”); if off-chain redemption fails while on-chain collateral remains “formally healthy,” dual-track depeg appears—audit on-chain C_0 separately from off-chain legal commitments.

Section 5. VRC-11 Protocol Functions and VRC Spectrum Interoperability

The blue paper splits VRC-11 capabilities into six module classes, forming Privcurrency’s closed loop from mint to payment.

Create (mint): enterprises or individuals holding Bitgold initiate minting through compatible interfaces; contracts lock collateral under 61.8% undercollateralization rules (stake ratio 61.8%) and issue private-domain stablecoins, permanently recorded on-chain.

Cross-chain payment: relying on Openverse underlying interoperability, Privcurrency can pass payment instructions and complete asset mapping among chains compatible with Ethereum, Polkadot, and others; the blue paper claims ability to bypass multi-correspondent cross-border wire chains—in reality paths still require compliance gateways, FX, and final fiat off-ramps; wholesale clearing and AML layers remain permissioned-system-led. Cross-chain links remain historically high-incident zones; deployment must separately assess bridge and routing-node trust assumptions—do not default to “safe” because of the word “cross-chain.”

Protocol swap: on Openverse’s decentralized trading layer, Privcurrency can auto-convert with VRC-10 (Bitcurrency), VRC-12 (Bitsecurity), and VRC-20 (fungible equity/points tokens) by market supply and demand. That lets enterprise private settlement units combine with public pricing, equity-type tokens, and internal points in one ecosystem—Treasury need not maintain isolated books for each asset class, but swap slippage and liquidity depth set practical boundaries.

On-chain consumption: Privcurrency can serve as DeFi lending collateral and as payment units for chain games and digital-rights markets; relative value stability avoids secondary FX risk from pricing in high-volatility native coins.

Offline payment: the blue paper plans merchant cooperation with QR or POS acquisition—off-chain experience approaching electronic payments, on-chain synchronized accounting. Landing depends on local licensing and tax treatment of crypto payment tools.

In-DApp payment: developers can integrate Privcurrency receipt at relatively low cost; after contracts verify payment validity they release digital services or permissions. Versus traditional payment gateways, advantages are fees and programmable splits; disadvantages are that fiat on/off-ramps and refund-dispute handling are not yet standardized.

Section 6. Structural Differences from USDT: Centralized Reserves vs On-Chain Collateral

Blue-paper Chapter 7 uses USDT as reference to highlight VRC-11 design trade-offs—this book selects structural comparison and does not credit promotional figures on market share or growth rates.

Dimension	USDT (typical fiat-collateralized stablecoin)	VRC-11 Privcurrency
Issuance right	Single institutions such as Tether	Anyone holding Bitgold may participate in minting via contracts
Value support	Bank fiat reserves + institutional promise	Bitgold undercollateralization (stake ratio 61.8%) + enterprise reputation and on-chain state
Transparency	Depends on third-party audits and institutional disclosure	Collateral and mint volumes theoretically verifiable on-chain
Main scenes	Crypto trading pairs, OTC dollar substitute	Enterprise private settlement, supply chains, cross-border B2B (design goals)
Regulatory touchpoints	Reserve quality, MSB licenses, securities-classification disputes	Private-domain KYC, payment/e-money classification, FX controls

USDT’ s advantage is liquidity depth and full exchange coverage—the de facto “on-chain dollar pipe”; VRC-11’ s advantage is customizable private-domain boundaries and multi-protocol combination within Openverse, not replacing USDT’ s generality in open markets. In enterprise selection, external settlement may still bridge via USDC/USDT while internal trade circles use Privcurrency—dual-layer structures are more common in practice.

Section 7. Linkage of Bitgold Stake Scale and Price (Theoretical Framework)

Blue-paper Chapter 8 builds a simple mathematical model relating Privcurrency mint volume to Bitgold price—this book introduces it only as an analytical framework and does not adopt extreme assumptions such as “150 countries abandon fiat, Fortune 2000 fully adopt” or the resulting thousands-of-dollars BTG price.

The model places into a supply–demand narrative: stablecoin mint scale S , stake ratio r (VRC-11 baseline 61.8%), stake lock period L , market-sentiment index α , and Bitgold circulating supply Q_s and demand Q_d . Core intuition: minting Privcurrency locks Bitgold; rising $S \rightarrow$ fewer tradable BTG on the market $\rightarrow$ upward price pressure if demand is unchanged; concentrated redemption reverses this. Longer stake periods lock BTG longer, with more lasting effects on float.

The blue paper also discusses positive feedback between market sentiment α and staking behavior: in optimism more agents willingly collateralize and mint; in pessimism they unlock and sell—isomorphic with crypto markets’ familiar “collateral spiral.” Implication for protocol governance: a single fixed stake ratio may be too loose or too tight across bull–bear switches; parameter adjustment and circuit-breaker mechanisms must be reserved rather than idolizing 61.8% as eternally optimal.

The model matters especially when VRC-10, VRC-12, and VRC-11 share Bitgold collateral: simultaneous multi-protocol expansion stacks collateral contention. Assessing the Openverse ecosystem should observe BTG stake shares across all three protocol chains, not Privcurrency alone.

Section 8. Enterprise Applications and Small-Country Scenes

Financial and enterprise scenes listed in blue-paper Chapters 4–5 can be grouped into three use classes (distinct from unverified marketing cases). Deriving industry penetration from narrative templates (e.g., “ABC Trading Co.”) commits the possibility→reality leap: success requires simultaneous whitelist, target-country non-prohibition of stablecoin settlement, compliant off-ramps, and off-chain redemption—incremental value must be proven under the same metrics (total cost, arrival latency, FX exposure, failure-retry rates), or technical advantage stays at the interface layer.

Cross-border payment and settlement: importers pay overseas suppliers in Privcurrency, aiming to compress fees and arrival time. Success conditions include: both parties on the permissioned whitelist, target country not forbidding stablecoin settlement, compliant off-ramp channels. Blue-paper “ABC Trading Co.” and similar are narrative templates; readers should demand actual launch data and audit reports.

Supply-chain finance: core enterprises stake Bitgold to mint Privcurrency and advance on-chain prepayments to suppliers; smart contracts auto-debit repayment after delivery. Consistent with Chapter 18 deployment paths; the key is whether core enterprises accept on-chain payable transparency.

Decentralized lending: Privcurrency holders may collateralize tokens in DeFi layers to borrow liquidity; rates are set by contracts and supply–demand. If Privcurrency is accepted as collateral by external CDP protocols (e.g., Maker-style lending pools), that protocol’s liquidation line L applies—this does not contradict VRC-11’s native mint rules setting no L/W ; risk comes from cross-protocol composition, not from Privcurrency minting itself.

Internal enterprise finance: the blue paper proposes Privcurrency as an internal unit of account, with expense reimbursement and budget allocation auto-reviewed and paid by smart contracts; blockchain traceability substitutes for part of manual review. Suited to multinational teams unifying an “internal dollar unit” and reducing multi-fiat friction; must coordinate with national labor law, tax withholding, and accounting standards.

Payroll: multinationals pay overseas employees’ wallets directly in Privcurrency, claiming to avoid bank queues and FX erosion. Real constraints include: whether employees’ countries treat it as taxable income, whether wages must be paid in local currency, social-security and housing-fund contribution currencies—technically reachable, institutionally not necessarily permitted.

Real-time inter-enterprise settlement: B2B goods trades settle in Privcurrency, synchronizing title transfer and payment, reducing forged instruments and account-period lockup. Versus traditional electronic payments, incremental value is programmable conditional payment (e.g., “auto-release after acceptance signature”), not mere speed.

Small-country scenes (cautious): the blue paper says resource-, trade-, and digital-oriented small economies can use VRC-11 to build digital payment networks and stabilize domestic purchasing power. Such narrative touches sensitive monetary sovereignty territory; this book records it as a protocol-layer “optional tool,” not a claim about any sovereign monetary policy. Feasible paths are more likely private-domain stablecoin pilots in offshore trade circles or special economic zones, parallel to domestic fiat—not “full fiat replacement”—Singapore, Kazakhstan, Estonia, and similar blue-paper cases are narrative demonstrations; they must be checked against those countries’ real regulatory documents and not treated as already-landed policy.

Section 9. Permission Boundaries, KYC, and the Blue-Paper Compliance Framework

Private-domain stablecoin boundary management relies on permission lists (whitelists): only KYC-certified addresses on specific lists may receive and send private-domain stablecoins. Smart contracts check whether

sender and receiver are whitelisted before every transfer; non-whitelisted addresses cannot participate. This mechanism lets private-domain stablecoins meet AML and KYC requirements with a clear technical compliance path.

On regulatory compliance, private-domain stablecoins may fall under multiple frames depending on function and participant type. If treated as payment instruments, payment-service licenses may be required; if as e-money, e-money issuance rules; if limited to specific uses in closed ecosystems (e.g., parks), prepaid-card or gift-card rules may apply more loosely. Applicable frames differ by jurisdiction—cross-border private-domain stablecoins must analyze each target market’s regulatory path rather than apply a single scheme.

Blue-paper Chapter 6 outlines Openverse’s compliance strategy (to be checked item by item against national law): multi-jurisdiction legal research; crypto and identity-authentication tech satisfying privacy and AML; token issuance and trading access review; dedicated compliance departments and periodic audits; regulatory dialogue mechanisms and policy-adaptation plans. For users, protocol-provided KYC whitelists, transaction monitoring, and report-export interfaces cannot replace counsel’s classification opinions—especially under divergent patterns such as MiCA (EU), US SEC/CFTC division, and China’s prohibition of virtual-currency businesses.

Another technical-compliance difficulty is the balance of privacy and traceability: public-chain transparency tensions with regulatory customer-data protection; zero-knowledge proofs and similar schemes try to compromise, but deployment maturity varies by chain. As a permissioned-domain tool, Privcurrency often chooses a hybrid architecture of “on-chain traceable + off-chain identity mapping,” with the issuing enterprise or park operator as data controller.

Section 10. VRC-12: Bitsecurity and Security-Type Token Issuance

VRC-12 (Bitsecurity) enters another functional layer: tokenizing enterprise equity or income rights into on-chain circulating security-type tokens. Its blue paper’s core logic is “asset anchoring + rights proof + compliant circulation.”

Enterprises stake Bitgold as collateral and issue Bitsecurity tokens, each mapping a specified share of equity or income rights. Technical advantages include: equity state inspectable on-chain without relying on a single registrar; peer-to-peer trading under compliant whitelists, lowering liquidity discounts of traditional private equity; smart contracts auto-executing dividends and buybacks, lowering trust costs of performance.

Dynamic stake ratios and liquidation mechanisms are the most complex parts of Bitsecurity design. If Bitgold stake value continuously exceeds Bitsecurity market cap, the system is healthy. If Bitgold price falls so stake value breaches set thresholds, margin calls or forced liquidation trigger. The logic matches DeFi CDPs (collateralized debt positions), but the object shifts from anonymous borrowing to enterprise finance.

Bitsecurity thus faces both on-chain risk (collateral-price volatility, liquidation-mechanism technical risk) and off-chain risk (legal force of equity, priority in enterprise bankruptcy, regulatory compliance). Smart contracts can execute on-chain-state logic but cannot replace legal systems’ confirmation of equity—if a Bitsecurity-issuing enterprise is liquidated off-chain, token holders’ legal rights depend on whether their jurisdiction recognizes on-chain proof and on issuance-contract terms. That is the fundamental challenge of the whole RWA (real-world-asset tokenization) track.

Section 11. RWA: The Global Wave of Real-Asset Tokenization

VRC-12 faces the global RWA tokenization track: mapping Treasury funds, corporate bonds, receivables, real-estate interests, commodity inventories, and more into on-chain representations. In 2023–2024, BlackRock launched tokenized fund BUIDL on Ethereum (live March 2024, AUM reaching hundreds of millions within weeks), Franklin Templeton continued its on-chain government money fund on Stellar, and JPMorgan’s JPM Coin/Onyx served institutional wholesale payments—all pilot products within regulatory frames, still small shares relative to traditional asset-management AUM⁴. BIS (2023) lists tokenized deposits and wholesale CBDC among next-generation financial-infrastructure options—not equivalent to on-chain RWA already replacing T+2 securities clearing or registration-system dominance—when narrating “institutions adapting to new settlement,” distinguish sandbox scale from mainstream-path substitution; long-run institutional co-evolution.

RWA tokenization’s core value claims include: raising liquidity of illiquid assets (private equity, property shares circulating in smaller units); lowering clearing and settlement time costs (traditional securities T+2 vs near-real-time on-chain); expanding potential investor sets (through compliant permission layers, opening asset classes once institution-only to broader accredited investors); and automating compliance checks and rights distribution via smart contracts (dividends, principal/interest repayment, voting).

Challenges are equally significant. Legal: most jurisdictions’ title systems rest on written registration and legal documents; how far on-chain tokens have court-recognized legal force differs and is still evolving. Technical: information channels between on-chain tokens and off-chain assets (oracles, reporting, custody) are the system’s most fragile link—any fraud or error can severely detach token value from underlying assets. Regulatory: security-type tokens almost inevitably trigger securities law, requiring registration exemptions or full registration and sharply raising issuance costs.

For VRC-12 to gain footing on this competitive track, it must pass simultaneously on compliance support, underlying-asset quality assurance, and user experience. Its Bitgold collateral mechanism is a differentiated path but also introduces risk exposures unlike mainstream RWA platforms—investors must understand they are exposed not only to underlying-asset risk but also to Bitgold price volatility.

Section 12. Common Logic of Collateralized Issuance and Systemic Risk

VRC-10, VRC-11, and VRC-12 all use Bitgold as value reserve and credit collateral. Differences lie in mapping objects: public fiat units (Bitcurrency) to VRC-10; enterprise private-domain stable settlement to VRC-11; enterprise-specific rights (Bitsecurity) to VRC-12. The commonality is issuance and collateral state observable on-chain—when implemented well, superior to black-box off-balance-sheet financing.

Parameter linkage: when the three protocols share a Bitgold collateral pool, Chapter 14 and Section 4’s C_0 and x^* apply simultaneously to VRC-10/11—any subsystem’s expansion reduces circulating BTG and synchronously tightens collateral coverage in downturns. VRC-12 sets independent liquidation thresholds. Assessing systemic risk requires summing BTG locked across all three protocols, then stress-testing with $C(x) = C_0(1 - x)$, not estimating protocols in isolation.

That commonality also concentrates systemic risk. If Bitgold prices fall sharply, they may simultaneously trigger VRC-10 Bitcurrency redemption runs, VRC-11 Privcurrency redemption runs, and VRC-12 Bitsecurity position liquidations (VRC-12 retains CDP-style thresholds); three subsystems synchronously generate Bitgold unlock or sell demand, further depressing Bitgold prices. Blue-paper Chapter 8’s linkage model under extremes describes exactly this collateral spiral; shared collateral creates cross-protocol systemic-risk transmission—when one subsystem is stressed, others sharing the same collateral are stressed in parallel.

Design responses include: independent collateral pools per protocol, preventing one subsystem's pressure from affecting another; introducing non-Bitgold diversified collateral, lowering single-asset volatility's systemic impact; establishing inter-protocol emergency pauses that temporarily stop new minting under extremes, slowing runs and (for VRC-12) liquidation-cascade speed.

Whether these mechanisms are already realized in the Openverse suite must be verified concretely from technical docs and on-chain contracts. The purpose here is to point assessment paths, not to conclude on particular implementation states.

When Maker-style $C < L$ triggers on-chain forced auctions (March 2020 ETH intraday drops ~30%+, zero-price auctions as empirical benchmark), collateral dumping can procyclically amplify price declines—Qin et al. (2021) longitudinal liquidation data show discounted sales often occur excessively at borrowers' expense⁵. When VRC-10 deliberately sets no L/W , the main pressure path becomes redemption runs rather than auction cascades; when VRC-10/11 redeem synchronously while VRC-12 triggers liquidation, BTG faces combined “unlock sell pressure + auction sell pressure,” and $C(x) = C_0(1 - x)$ tightens all three layers at once (Section 4 numerical example: VRC-11 at $x = 20\%$ has $g = 50.6\%$ —cannot apply VRC-10's $\delta \leq \varepsilon$ upper bound). When thin-pool TWAP is manipulated or OTC depth is insufficient (Ferraro et al. 2022; Ahmed et al. 2024 reserve-disclosure paradox), even readable on-chain C_0 may see pegs deviate as redemption queues lengthen—the oracle chain must join arbitrage chains and market depth². Independent collateral pools, diversified collateral, and inter-protocol emergency pauses are design options; S&P Global (2023) and Chitra et al. (2024) DAISIM show that even overcollateralized CDPs' peg-deviation duration moves with OTC depth and belief parameters—VRC-11 “dual-track depeg” when off-chain redemption fails must enter the same frame. Open questions remain: three-layer BTG contention is PCIM's incremental challenge relative to single-protocol Maker—not a solved problem.

Section 13. Regulatory Interaction: The Intersection of Securities and Payment Law

Landing VRC-11 and VRC-12 inevitably enters multiple regulatory intersections. Private-domain stablecoins involve payment regulation; security-type tokens involve securities regulation; if they circulate cross-border, FX controls and cross-border capital-flow rules also apply.

For enterprises, issuing or using private-domain stablecoins requires counsel-guided analysis: how does the target jurisdiction classify the instrument (payment voucher, e-money, security, other)? What licenses or exemption paths are needed? How are AML duties implemented (monitoring, suspicious reporting, user authentication)? What ongoing disclosure duties exist? There are no universal answers; each market must be analyzed.

Protocol-layer design should supply necessary compliance interfaces rather than push all compliance responsibility onto users. A mature VRC-11 implementation should embed KYC whitelists, transaction limits, and compliance-report export; VRC-12 should support investor-suitability management (accredited-investor certification), disclosure modules, and shareholder-register export so issuers can meet securities compliance. Standardizing these interfaces at the protocol layer not only lowers single users' compliance costs but also makes the protocol more scalable—the more complete the compliance interfaces, the wider the legally usable scenes.

Section 14. The Long Narrative of Assets On-Chain: From Digitization to Programmability

Asset tokenization is an acceleration phase in the long digitization of monetary and financial infrastructure—not a sprint. Historically, financial-asset representation evolved over decades from physical forms (gold/silver, paper instruments) to electronic records (bank accounts, securities registries). Tokenization is the next layer:

atop electronification, adding programmability—assets can embed rules, auto-execute, and combine with other protocols, no longer only static rights proofs.

A token holding government-bond shares can simultaneously serve as DeFi lending collateral; a tokenized receivable can be transferred repeatedly in supply-chain finance networks; a tokenized equity can auto-distribute dividends to holders via smart contract—without multi-layer intermediaries of brokers, clearinghouses, and registrars. That programmability is tokenization’s true incremental value relative to traditional electronic securities.

VRC-12’s design tries to capture that incremental value at the technical layer. Success ultimately depends on whether it can keep on-chain programmable advantages while meeting off-chain legal systems’ formal confirmation of title. Protocols alone cannot solve this; they need legislative innovation at the jurisdiction level and continuing dialogue and adaptation between financial regulators and blockchain protocols.

Section 15. Private-Domain Stablecoin Interoperability: From Closure to Connection

If private-domain stablecoins forever circulate in a single private domain, their network-effect ceiling is extremely limited. True incremental value lies in private-to-private and private-to-public interoperability. When two different supply-chain private networks must settle and use different private-domain stablecoins, they face a “cross-domain exchange-rate” problem: how is the conversion ratio set? Who market-makes? Do FX frictions eat the costs private-domain stablecoins were meant to save?

IBC (Inter-Blockchain Communication) and VTP (Value Transfer Protocol) supply infrastructure-layer design possibility for this problem. If two private networks both access Openverse Layer 0 value-exchange layer (ecosystem Layer 1 app chains or external chains bridged via IBC/VTP) and both are willing to open mutual recognition, cross-domain settlement can, per white-paper design, complete at the protocol layer without always falling back to fiat—reality still depends on both sides’ compliance permissions, FX, and liquidity depth. Section 4’s VRC-11/VRC-10 swap functions let private-domain stablecoins and public Bitcurrency migrate value when compliance and pool depth allow without fiat intermediation.

Expanding cross-private interoperability must also proceed within compliance frames. If two private networks register in different jurisdictions, cross-domain transfers may trigger FX-control rules requiring regulatory reporting. That means private-network interoperability protocols are not only technical protocols but also agreements on both sides’ compliance duties. When designing private-domain stablecoin interoperability, compliance-reporting paths must be designed in parallel so cross-domain flows are traceable and supervisable.

Section 16. Bitsecurity Valuation Logic and Holder Analysis

As a hybrid of enterprise rights and Bitgold staking, Bitsecurity’s valuation is more complex than traditional stocks: holders must simultaneously assess underlying enterprise-asset value, Bitgold stake-position health, and on-chain liquidity’s effect on token price.

From the underlying-enterprise-asset angle, Bitsecurity valuation resembles traditional private equity: DCF or comparable-transaction multiples, but with token liquidity premiums or discounts (if tokens transfer more easily than private shares, a liquidity premium; if holders face high information-acquisition barriers, an information-asymmetry discount). Bitgold stake health is an extra valuation factor: if Bitgold prices approach liquidation thresholds, Bitsecurity’s effective stake protection weakens, token risk rises, and rational holders must reflect that extra exposure in valuation.

Diversity of holder types and motives shapes Bitsecurity secondary-market behavior. If holders are mainly long-term value investors, token liquidity is lower but prices relatively stable; if mainly arbitrage traders, volatility is larger but liquidity stronger; if institutions enter, stronger information processing lowers asymmetry discounts but also accelerates price discovery, making prices react faster and more violently to bad news. Issuers designing circulation mechanisms, investor-relations strategies, and governance rules must first map holder structure.

Section 17. Long-Run Dynamic Relations Between Private and Public Domains

Private and public domains long interact dynamically rather than as a static dichotomy. Today's private-domain stablecoin, if adoption is wide enough, may gradually gain acceptance beyond its initial permissioned domain and evolve toward the public; today's public currency, if governance introduces participation limits, may locally contract toward the private. That dynamism means protocol classification should not be a one-time label but continuous tracking of actual circulation patterns and acceptance-circle boundaries.

For regulators, private-public dynamics blur regulatory borders: tools once exempted for "private-domain closure," if actually circulating widely in the public domain, invite regulatory intervention. On-chain inspectable address distributions can, per white-paper design, supply harder factual bases than pure self-reporting—but must be read with privacy rules, off-chain identity mapping, and mixer/cross-chain splitting; whether they convert into effective enforcement tools depends on whether jurisdictions recognize on-chain records' force—pending case law and mature compliance interfaces; do not presume "regulatory advantage already established."

Private-public dynamic evolution in some degree recapitulates the ancient monetary-history process of "how private money gains wider acceptance." From medieval bills of exchange circulating in particular merchant networks, through expanding bill-discount markets, to modern commercial-bank deposits' generalized acceptance—each "private-domain money becoming quasi-public" accompanied credit expansion, regulatory adaptation, and institutional innovation. VRC-11 and VRC-12 trajectories will not simply repeat that history, but monetary history's experience of private instruments diffusing to wider acceptance circles still helps anticipate their direction and institutional challenges. For participants, understanding the institutional experiment they join with historical vision is not only intellectual honesty but risk-management necessity.

Section 18. Time Commitments and VRC-13

Protocol representation of time-class assets appears in Chapter 16 (VRC-13 Time Token). This chapter focuses on private-domain stability and assets on-chain and does not repeat time-token mechanism design.

Section 19. Institutional Complementarity: Non-Technical Conditions of Protocol Success

A through-line of this chapter is that technical sophistication of protocols is necessary, not sufficient. Private-domain stablecoins need robust issuance mechanisms, compliant permission frameworks, interoperability interfaces with existing finance, and real enterprise participants who can use and understand them; security-type tokens need legal title confirmation, disclosure, investor protection, and judicial systems willing to recognize on-chain records' force. These "non-technical conditions" often mature slower than technology itself, creating systemic risk of institutional lag.

Institutional complementarity is widely used in comparative economics: an economic system's performance depends on coordination among institutional components; upgrading a single component does not guarantee system-wide improvement and may even produce negative effects from mismatch with others. On-chain protocols are novel institutional components; their complementarity with legal systems, regulatory frames, accounting

standards, and enterprise capabilities determines actual efficacy. In markets where complementarity conditions are immature, forcibly pushing advanced protocols may backfire.

The right strategy is, while advancing technology, to participate actively in building institutional complements: dialogue with legislatures to push legal recognition of on-chain assets; cooperation with accounting-standard setters to supply practice cases and expert opinion on tokenized-asset accounting; joint design of compliance paths with regulators rather than waiting for forced enforcement and then reacting passively. This “technology–institution co-evolution” strategy is a common feature of several past successful financial innovations—whether the VRC protocol suite can reach large-scale landing still depends on how fast complementarity conditions mature.

Section 20. The Historical Place of Private-Domain Financial Innovation

The complexity of private domains and assets on-chain maps real commercial environments, not obstacles that can be bypassed. For protocol developers, compliance interfaces should be written into design cores; for corporate treasurers, regulatory classification and legal opinions must be completed before adopting VRC-11 or VRC-12—do not copy others’ paths blindly; for policymakers, on-chain visibility supplies new regulatory tools worth exploring rather than uniformly applying old frames; for investors, clarifying where risk hangs is the minimum threshold for participation.

On a longer historical arc, private-domain financial instruments have always been the most active sites of financial innovation. From medieval merchant-guild internal credit notes, through modern commercial-paper markets, to twentieth-century asset securitization—each innovation began in the private domain and, after gradually expanding acceptance circles, formed wider market influence. VRC-11 and VRC-12 likewise start from the private domain; their future trajectory will be jointly decided by market forces, regulatory wisdom, and ecosystem-building capacity—private-domain financial innovation has always begun within boundaries and then gradually widened acceptance; that journey has only just begun.

注释与引用

1. MakerDAO Purple Paper (2019, source: official technical white paper, not independently audited): CDP collateral ratios and liquidation line L / warning line W ; Black Thursday Post Mortem (2020-03-12): post-event raising of ETH minimum collateral ratios; MakerDAO Endgame Litepaper (2023-03, source: official Litepaper v1, not independently audited): SubDAO split and MKR governance restructuring. <https://endgame.makerdao.com/> ; Auer, Cornelli & Frost (2022), *BIS Quarterly Review* December issue, pp. 69–82: DeFi lending-parameter governance cases. ↩
2. Viswanath-Natraj, Ganesh, and Richard K. Lyons. "Stable coins don't inflate? On the dynamics of USDC pricing." *Journal of International Money and Finance* 131, 2023, 102777: fiat-reserve stablecoin stress discounts; Lyons & Viswanath-Natraj (2020), NBER WP 27136: reserve-redeemability framework; Grobys, Klaus, et al. "On the stability of stablecoins." *Journal of Empirical Finance* 64(C), 2021, pp. 207–223: peg-deviation panels; Brauneis, Alexander, et al. "How stable are stablecoins?" *European Journal of Finance* 30(9), 2024, pp. 1027–1058: thin-market peg deviation; Ferraro, Kan & Sunderam (2022), Princeton Economics WP 1416: thin-market peg fragility; Ahmed, Aldasoro & Duley (2024/2025 rev.), BIS WP 1164: reserve-disclosure paradox (P5 proposition). <https://doi.org/10.1016/j.jimonfin.2023.102777> ; <https://doi.org/10.1016/j.jempfin.2021.09.002> ; <https://doi.org/10.1080/1351847X.2023.2240254> ; <https://www.bis.org/publ/work1164.htm> ↩ ↩² ↩³
3. Klages-Mundt et al. (2023), *Journal of Financial Stability* 68, 101142: algorithmic stablecoin vs overcollateralized CDP risk boundaries; Arner, Buckley & Schularick (2022), *Journal of Financial Regulation* 8(2), pp. 155–179: stablecoin regulatory classification and mechanism comparison. ↩

4. BlackRock (2024-03), USD Institutional Digital Liquidity Fund (BUIDL) live on Ethereum; Reuters (2024-03-21) reported AUM reaching hundreds of millions within weeks of launch. Franklin Templeton, OnChain U.S. Government Money Fund (Stellar, from 2021). JPMorgan, Onyx/JPM Coin institutional wholesale payments (from 2020). BIS (2023), *The Future Monetary System* (Annual Economic Report, Chapter III), §III.B: tokenized deposits and unified ledgers as next-generation infrastructure options, not a claim of mainstream-path substitution. <https://www.reuters.com/technology/blackrocks-tokenize-d-fund-ethereum-2024-03-21/> ; <https://www.bis.org/publ/arpdf/ar2023e3.htm> ↩
5. MakerDAO Risk Team (2020-03-12), “Black Thursday Post Mortem”; Gudgeon et al. (2020), “DeFi Protocols for Loanable Funds,” *AFT* 2020: liquidation auctions and procyclical mechanisms; Eisenberg & Schär (2021), “DeFi Liquidations,” *AFT* 2021: liquidation discounts and MEV extraction. Section 12 “liquidation cascade vs redemption run” contrast appears in the main text. ↩

§ 16 Time as an Asset

VRC-10 through VRC-12 cover public currency, private-domain stability, and asset securitization; this chapter completes the final layer of the protocol spectrum. VRC-13 (Time Token) tokenizes time resources—professional service hours, project durations, service commitments—so they can be quantified, transferred on-chain, and verified in use. Conceptual boundaries, protocol design, the border with money, placement in the value internet, and institutional and legal challenges must all be discussed within this frame.

Section 1. The History of Commodifying Time

Before industrialization, most people's time was not precisely priced by the hour. Agrarian societies measured labor by season; crafts paid by piece; services scarcely formed a system. The Industrial Revolution changed that: factories paid by the hour; Taylorism (scientific management) dissected and metered labor time precisely; the monetization of time entered a phase of full acceleration.

In the second half of the twentieth century, the rise of services pushed time pricing to higher complexity. Lawyers bill by the hour; consultants charge day rates; physicians' time is priced indirectly through consultation fees; a speaker's single-engagement fee is hard to map to a simple "hourly equivalent." In professional-service markets, time pricing is both a meter of labor value and a bargaining game under information asymmetry.

The digital economy further subdivides time's granularity: cloud computing bills by the second; advertising pays per thousand impressions; gig platforms (Upwork, Fiverr) settle per job; livestream tips correspond to creators' instantaneous attention. Every commercialization of time depends on underlying metering, recording, and settlement infrastructure. Yet that infrastructure is highly fragmented: each platform builds its own timers, balance accounts, and dispute mechanisms; cross-platform time assets are neither transferable nor composable.

VRC-13 confronts exactly this fragmentation. If professional-service "time commitments" can be uniformly represented as on-chain tokens—recognizable and transferable across platforms, mortgageable and composable when embedded in DeFi—then time upgrades from a number on isolated platform ledgers to a native asset class of the value internet. The Openverse white paper also lists "Timing Token" separately in its asset taxonomy, with standard code VRC-30, defining validity intervals by main-chain block height for device-use rights, time-limited voting, and similar scenes; the text below follows the VRC spectrum as VRC-13 (Time Token)—when consulting official documents, note version and numbering correspondence.

Section 2. A Conceptual Framework for Time Tokenization

A Time Token framework must answer four sets of questions: what rights the token represents; how rights trigger and consume; how fraud is prevented; how disputes are handled.

The most basic reading is "one token equals a purchase right to one unit of service time." The unit may be an hour, a day, or a full cycle of a specified service. The holder may claim the corresponding service from the issuer (service provider); after completion the token is consumed (burned or marked completed). The logic matches gift cards and prepaid service vouchers; the difference is that on-chain records make rights state independently verifiable without trusting a single issuer's database.

How off-chain events—timing start (service begins) and timing stop (service ends)—map to on-chain state is the critical technical problem. For physical services (in-person consultation), on-chain mechanisms can scarcely sense duration automatically; for digital services (online tutoring, SaaS usage, API call counts), contract

callbacks or oracles can write digitized timing data on-chain. Different service types require different technical paths; there is no universal silver bullet.

The core anti-fraud challenge is preventing “double sale”—the same time slot promised to two different buyers. Under an on-chain token frame, if the issuer mints a corresponding token for each time unit and total supply is tied to actual available capacity, double sale is detectable on-chain. Consistency between off-chain promises (oral, contractual) and on-chain records still requires off-chain legal constraints.

When service quality falls short of agreed standards, how do holders assert rights? Smart contracts can record claims but cannot assess subjective judgments such as “whether one hour of consultation met the promised level.” Off-chain arbitration or dispute resolution remains indispensable; protocol design must reserve interfaces for that complement rather than assume all disputes resolve automatically through on-chain logic.

Section 3. Individually Issuable Credentials: The Time Dimension of Popularization

In the narrative of monetary popularization, time tokens represent a distinctive dimension of falling participation thresholds: individuals can issue service credentials backed by their own time.

Traditional monetary issuance belongs to the state—the central bank is the sole lawful issuer. Private banks create credit money, but only within the central-bank frame and with licenses. Even Hayek’s vision of private monetary competition presupposed capitalized institutions as issuers; individual self-issuance of **general-purpose** money was nearly impossible in the paper era. PCIM extends competitive public-currency issuance to any participant holding Bitgold—beyond the institutional threshold of Hayek’s time, yet still issuance under collateral-mint rules, not unconstrained personal printing; it must be narrated separately from time tokens below.

Time tokens open another path: individuals can treat future service time as value backing and issue service credentials within Openverse or similar open-protocol frames. These credentials are not money in the legal sense, but they have exchange value within particular acceptance circles—just as gift cards, hour-swap contracts, and service contracts have value; time tokens are on-chain upgrades of those traditional value carriers. Individuals issuing standardized credentials backed by their own time is like reconstituting professional services as transferable standardized vouchers—one on-chain representation of long-tail labor time.

“Falling participation thresholds” gains more concrete meaning here: ordinary people cannot join central-bank monetary policy, but professionals can standardize service-time commitments as on-chain assets circulating in circles of trust. This decentralization supplements the fiat system rather than replacing it—it brings long-tail assets (individual professional time) previously unserved by finance into the representable and transferable range of the value internet.

Of course this requires real service capacity and willingness to perform on the issuer’s side, and capacity to assess quality on the acceptor’s side. On-chain tokens solve the “transferable rights credential” problem; whether the right is worth holding still depends on the issuer’s real credit. Reputation mechanisms—on-chain rating systems or off-chain word of mouth—are necessary complements to the time-token ecosystem, not optional decoration.

Section 4. The Blurring Boundary Between Time Tokens and Money

There has never been a clear natural boundary between “money” and “non-money”; society’s acceptance, legal classification, and historical custom jointly define it. Points, gift cards, prepaid cards, travel miles, and game currencies all have monetary functions to varying degrees (store of value, medium of exchange) yet are classified by law as “non-money.”

Where do time tokens sit on this spectrum? If an enterprise that frequently uses a professional's services pays advances in time tokens, books them in accounts payable, and circulates them internally—that already approaches “private-domain money.” If time tokens are widely accepted as deferred-payment units in a large enough professional-service market, with circulation velocity and acceptance depth at sufficient scale, their monetary functionality becomes hard to ignore.

Whether something becomes money depends on acceptance-circle scale and clearing depth, not on the issuer's self-label. That judgment matters especially for regulators: if a token class actually performs monetary functions while calling itself a “service credential” to evade regulation, regulators must classify by function rather than form. Many jurisdictions already develop substance-over-form rules in this direction—whatever you call it, if it is used to buy things, pay wages, or store value, regulators treat it under monetary rules.

For VRC-13 designers, functional restraint may have strategic value: designing use credentials within specific service circles rather than general media of exchange can lower the risk of being classified as money (and thus triggering monetary regulation). Yet if the ecosystem prospers enough, that restraint may ultimately fail to prevent substantive monetary functions from forming—dialogue with regulators will then be inevitable.

Section 5. Collaboration with VTP and IBC: Time Assets Enter the Value Internet

The Value Transfer Protocol (VTP) is the routing standard of Openverse's Layer 0 value-exchange layer, analogous to HTTP on the internet: standardizing transfer, addressing, and settlement paths among asset types to lower frictions of cross-protocol and cross-Layer 1 interaction. Inter-Blockchain Communication (IBC) supplies communication infrastructure for asset transfer among different blockchains, analogous to interconnection among national telecom networks—external Layer 1s can access Openverse Layer 0 via IBC or VTP rather than only running inside closed subnets.

Isolated time tokens have limited use: if an engineer's time tokens can circulate only in a small Openverse circle, liquidity discounts and issuance costs make them economically unattractive. But if time tokens can circulate more widely through VTP and IBC—accepted as DeFi collateral, used in cross-chain settlement, recognized as standard assets in other chains' applications—liquidity rises significantly and holders have more choice.

Realization has several premises. Time tokens must meet cross-chain recognition standards: on-chain metadata (issuer information, service type, validity, unit definitions) must be standardized for automatic parsing by other systems. Time tokens need enough trading depth to be accepted as valuable DeFi collateral—otherwise protocols refuse them for price-manipulation risk. Redemption mechanisms must be transparent and reliable, or liquidity collapses instantly under stress.

If these three conditions are gradually met, time-class assets evolve from “exclusive service credentials” into a “native asset class of the value internet,” standing alongside money, equity, and bonds as globally circulating and composable value representations. That vision awaits ecosystem maturity; releasing the VRC-13 standard alone does not deliver it.

Section 6. Institutional Tension: Labor Law and Time Assets

Time tokenization is technically feasible yet faces multilayered legal tension.

Labor-law perspective: if an employee's work time is tokenized and paid as tokens, wage-payment rules (e.g., minimum wage in legal tender), employer social-security contribution bases (how to compute bases in

tokens), and labor-law limits on “payment in kind” may trigger. Jurisdictions differ greatly, but the general trend is that replacing any part of statutory-currency wages requires satisfying corresponding rules.

Consumer-protection perspective: purchasers of prepaid service tokens need consumer-rights protection—if the issuer (service provider) cannot perform, how do buyers obtain refunds? Prepaid consumption is explicitly regulated in many jurisdictions—refund rights, reasonable-term requirements, prepaid-amount caps, and so on. If time tokens are treated as prepaid service vouchers, these rules may all apply.

Tax-classification perspective: does issuing time tokens constitute a taxable income event? Does purchasing constitute asset acquisition? Must token appreciation pay capital-gains tax? Must using tokens to redeem services report VAT or service tax? There is no global uniform answer, but each participant needs clear guidance in their own tax jurisdiction to participate safely.

These tensions do not doom time tokenization; they show that large-scale landing must proceed in parallel with institutional construction—either finding clear compliance paths within existing law or pushing adaptive regulatory adjustment. Technical protocols can go first; if institutional complements remain long absent, scaled use stays in legal gray zones and cannot form a lawful, transparent market.

Section 7. Pricing Time Assets and Liquidity Markets

If time tokens truly form a market, their pricing mechanism becomes an interesting economic question. Different providers’ time units are nominally all “one hour,” yet markets should price them very differently: top lawyers’, senior surgeons’, and popular artists’ time tokens will trade far above ordinary providers’.

VRC-13 is homogeneous at the interface layer (same standard, composable calls) and heterogeneous at the economic layer: Time Tokens from different issuers have sharply different values and cannot swap 1:1—aligned with ERC-721 NFT logic: same formal appearance, each backing a different value proposition.

If time tokens are priced per issuer, the pattern is “each service provider owns their own time-token market,” akin to personal tokenization of celebrities or IP. Liquidity will be highly fragmented—each market small, market-making costly, buyers and sellers hard to match.

Possible paths out of liquidity fragmentation include: pooling time tokens by “service category”—aggregating like tokens for “programming time,” “design time,” “legal consulting time” to raise liquidity; tiering issuers by platform credit ratings with limited interchange among same-tier tokens; and building renewal and expiry mechanisms so large volumes of “expired” tokens do not long occupy markets unused, creating false liquidity.

Liquidity-market maturity determines whether time tokens can truly become “native assets of the value internet.” If secondary markets stay thin, time tokens remain at one-to-one private-trade levels and cannot exploit protocol-layer scale advantages.

Section 8. Prospects in Education and the Knowledge Economy

The knowledge economy is the most promising soil for time tokens. In the traditional economy, knowledge work is extremely hard to standardize: one hour of a top programmer versus a junior may be priced tenfold apart. That gap makes knowledge-work pricing highly individualized and prevents deep secondary markets.

If time tokens combine with knowledge-worker credit assessment, layered markets can form: workers of different ability levels issue differently priced time tokens; in markets with enough liquidity these price by quality; buyers can compare time costs and historical performance records for more informed procurement. That is more transparent than traditional intermediary platforms—which usually control pricing strongly—whereas decentralized-market pricing is set directly by buyers and sellers.

Education has special appeal. Pre-purchasing teachers' teaching-time tokens can lock future service slots while giving teachers prepaid cash flow relief. If tokens can transfer among students who need them, allocation efficiency of educational services can improve: a student who bought but no longer needs a teacher's hours can transfer or sell tokens to others rather than simply lose the advance—social value for allocating high-quality educational resources.

Of course educational quality assessment is far more complex than ordinary goods; student feedback is shaped by many non-service factors (e.g., the student's own effort), so reputation mechanisms based on ratings more easily generate disputes in education. Time-token use in education needs relatively mature dispute resolution, or quality disputes will become the main barrier to user confidence.

Section 9. A Philosophical Dialogue with Labor Theories of Value

At a deeper level, time tokenization touches an old economic question: the labor theory of value. Marx held that commodity value is determined by socially necessary labor time expended in production; Ricardo earlier also took labor time as the foundational measure of value. That tradition treats time as the essential meter of value—an intriguing surface resonance with time tokenization.

Yet mainstream modern economics has long shifted to “marginal utility”: value is not determined by labor time but by subjective marginal utility. The same hour has sharply different value to different people in different scenes and demand states. In *The General Theory*, Keynes also stressed expectations and marginal efficiency as central to investment pricing—value discovery depends on market participants' subjective judgment, not mechanical conversion of objective labor time¹. Time-token markets embody marginal utility rather than labor value: a top expert's hour token trades at high prices because markets subjectively value scarce professional capacity highly—not because more “socially necessary labor time” was expended.

This philosophical contrast reminds us: time tokens do not solve the ancient problem of “how to meter human labor value fairly”; they only supply a more transparent market mechanism for subjective value to be discovered and equilibrated at larger scale. Their instrumental significance is real; their power to answer “the essence of value” does not differ fundamentally from ordinary goods markets. What monetary popularization promises is lower participation thresholds and trust costs for value exchange—not a fairer labor-metering method.

Section 10. Formalizing Informal Economies Through Time Assets

Complete standards are only a possibility base; real value requires enterprise adoption and institutional complements. Billions of workers worldwide labor in informal economies—no contracts, no social security, no credit history. Their labor time truly occurs and has real value, yet lack of formal records keeps them outside finance. If informal participants can record service-delivery history with on-chain time credentials, those records become the starting point of a credit file—not depending on bank accounts, employer certificates, or any centralized endorsement, only on verifiable on-chain behavior. That is the application potential of monetary popularization among the most marginal populations—and the direction most needing coordination with social policy and legal reform. Technically, VRC-13 here is only an enabling tool, not a complete solution; for informal participants truly to benefit, governments and regulators must recognize the legal force of on-chain records, and experience must be optimized for bottom-tier users.

Section 11. Combining Time Assets with DeFi Experiments

If time tokens enter mainstream DeFi liquidity pools, a series of interesting financial experiments become possible. The most direct combination: time tokens as lending collateral for stablecoin liquidity. Professional

service providers can then advance part of earnings as working capital before delivery—a decentralized version of traditional factoring, except collateral shifts from receivables to service-commitment tokens. MakerDAO-style overcollateralized CDPs lending DAI have run on mainnet for years²; yet applying the same template to time tokens must face the “thin markets” problem Ferraro et al. (2022) stress—stablecoin pegs themselves are fragile when OTC depth is insufficient³.

Realization must solve several critical problems. **Collateral valuation:** how do DeFi protocols price time tokens? Unlike stablecoins’ fixed prices or ETH’ s liquid quotes, time-token market prices depend heavily on issuer reputation and performance history—hard for on-chain oracles to fetch reliably. **Liquidation mechanisms:** if borrowers cannot repay, how are liquidated time tokens disposed of? Can third parties legally assert the service rights? Mature DeFi asset classes have standard answers; time-class assets need redesign. **Maturity matching:** time tokens usually have specific validity; lending protocols must ensure reasonable slack between loan maturity and token expiry, or produce unenforceable expired collateral.

These challenges are not insurmountable, but they need dedicated protocol design rather than direct reuse of existing DeFi templates. For VRC-13 to gain real DeFi liquidity support, the standard must incorporate lending-relevant metadata—issuer rating information, standardized service-type classification, validity and performability state—so DeFi protocols can handle time-class assets in standardized ways. That is work of technical-standard setting and ecosystem coordination, to be advanced in early dialogue between the Openverse suite and external DeFi protocols.

Section 12. The Philosophical Implications of Temporal Sovereignty

Philosophically, time tokenization touches a deep question: what temporal sovereignty—individuals’ autonomous command over their own time resources—means in the digital economy.

The rise of platform economies has, on one hand, raised the efficiency of monetizing personal time (Uber drivers flexibly schedule driving; freelancers take global platform jobs) and, on the other, brought algorithmic control over personal time (platform algorithms set dispatch frequency, pricing bands, acceptance pressure). Formal freedom of time use expands; substantive constraints of a new kind appear.

If time tokens truly achieve “individual issuance, individual pricing, peer-to-peer trading,” they will to some degree restore individuals’ pricing sovereignty over their own time: quotes set by individuals, buyers free to choose, time value no longer wholly decided by platform algorithms. That sovereignty is not unlimited—market competition still constrains pricing space—but “constrained by protocol rules” versus “constrained by platform algorithms” structurally approaches price competition in free markets rather than price-taking under platform monopoly. In *A Tract on Monetary Reform*, Keynes distinguished short-run disturbances of monetary reform from long-run stability—expansion of personal time-pricing power likewise needs balance between short-run trial-and-error and long-run institutional recognition.

This philosophical implication occupies a special place in the institutional evolution of time resources: it shows that popularization is not only about who can issue money, but also about who can define their own labor value and who can exchange value with others without depending on centralized platforms. Time tokens are a concrete technical carrier of that autonomy pursuit—though still quite far from large-scale application.

注释与引用

1. Keynes, 1936, *The General Theory of Employment, Interest and Money*, Chs. 11–12: marginal efficiency of capital and the central role of expectations in investment pricing. Marxists.org English text: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/> ↩
2. Schär (2021), *Federal Reserve Bank of St. Louis Review* 103(2), pp. 153–174: MakerDAO/DAI CDP and on-chain governance overview; MakerDAO Purple Paper (2019, source: official technical white paper, not independently audited): liquidation-line L / warning-line W design. <https://www.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> ↩
3. Ferraro, Kan & Sunderam (2022), Princeton Economics WP 1416 “Stable Coins but Thin Markets”: pegs more fragile when OTC depth is insufficient; Lyons & Viswanath-Natraj (2020), NBER WP 27136: reserve redeemability. <https://www.princeton.edu/~kan/StableCoins.pdf> ↩

Part V: Enterprise Management and Value Networks

§ 17 Corporate Finance and Multi-Currency Management

When a CFO faces a balance sheet that holds dollars, euros, renminbi, USDC, Bitgold, and Bitsecurity (VRC-12 equity-type tokens) side by side, the questions are liquidity allocation, accounting entries, tax filings, and FX hedges—a set quite unlike those in a protocol whitepaper. Treasury must fold positions in VRC-10 (Bitcurrency) and PCIM (Public Currency Issuance Mechanism), VRC-11 (Privcurrency), VRC-12 (Bitsecurity), and VRC-13 (Time Token) into a single liquidity-and-risk framework.

Section 1. The Historical Evolution of Corporate Treasury

“Treasury” (the finance or cash-management function) has long been a quiet but critical department in large firms. Its core duty is to ensure that at every moment the company has enough liquid funds to meet its obligations, while maximizing returns on idle cash through prudent asset allocation and managing exposures to FX, interest rates, counterparties, and the like.

Before globalization, corporate finance was relatively simple: most business stayed inside a single currency area, and bank-account management plus short-term bond investment exhausted Treasury’s work. Globalization forced multinationals into multi-currency cash management, cross-border cash pooling, FX hedging, and other complex operations. A manufacturer might buy raw materials in the dollar zone, sell finished goods in the euro zone, and pay wages in the renminbi zone; fluctuations among the three currencies became a standing financial risk.

The rise of digital payments and crypto assets layered further complexity onto multi-currency management. When firms began accepting crypto payments, settling cross-border flows in stablecoins, and holding bitcoin or ether as reserve assets, accounting treatment, tax reporting, and risk management all became markedly harder. This has long been a reporting and regulatory topic: Microsoft disclosed in its 2024 quarterly filings holdings of roughly 19,000 bitcoin (via affiliated funds); MicroStrategy treats bitcoin as a core treasury asset; Tesla, Block, and others have also disclosed positions. Consumer giants such as Nike, though they do not hold crypto, must still hedge revenue exposures in dozens of currencies each year. Multi-currency frameworks and on-chain settlement needs thus coexist in multinationals, drawing wide attention from auditors, regulators, and investors.

For firms in the Openverse ecosystem, the multi-currency environment often appears at once: fiat reserves; USDC/USDT and similar stablecoins (buffers for cross-border settlement); Bitgold (collateral for PCIM or VRC-12 staking); issued Bitsecurity (mapping the firm’s or affiliates’ equity); and protocol incentive tokens. Treasury’s question therefore shifts from “whether to touch on-chain assets” to “how to fold VRC protocol positions into a unified liquidity-and-risk framework.” The positions Treasury manages must still connect to production, sales, and receivables collection—not a self-contained loop detached from the real economy.

VRC-11 Privcurrency has several enterprise uses the bluepaper emphasizes, complementary to external supply chains. Cross-border teams may pay part of compensation in firm-minted private-domain stablecoins (such as MicroUSD)—fast on-chain credit, but individual tax withholding, social-security currency, and employee off-ramp compliance must still be solved. Budget lines, expense claims, and inter-department settlement may likewise be denominated in Privcurrency, with smart contracts disbursing by rule, cutting manual review and multi-fiat back-and-forth while leaving an auditable on-chain trail. With long-term partners inside a permissioned whitelist, the same Privcurrency unit can complete B2B delivery, binding title and payment in programmable form. The CFO must include these positions with VRC-10 public currency and fiat bank accounts in liquidity forecasts—Privcurrency minting locks Bitgold, and redemption unlocks BTG; VRC-12 Bitsecurity, by contrast, triggers on-

chain liquidation that sells BTG when the collateral ratio falls through a threshold. Both risk types share the same lineage as the linkage model in Chapter 15, Section 6, and must not be conflated.

Section 2. Accounting Frameworks for Crypto Assets

Accounting for crypto assets has been a priority for the major standard-setters (IASB, FASB) in recent years—and one of the practical headaches CFOs feel most acutely.

The principal global frameworks take different paths. Under IFRS, crypto assets are usually classified as intangible assets (IAS 38), measured at historical cost, written down only on impairment, with price increases not recognized in profit or loss—so a firm holding bitcoin that appreciates sharply does not reflect that gain in the income statement, yet must recognize losses immediately on impairment. That asymmetry hits crypto-holding firms' balance sheets disproportionately in down markets.

U.S. GAAP historically followed a similar path, but ASC 350-60, issued by the FASB in late 2023, now allows fair-value measurement of crypto assets, with changes flowing through earnings¹. That is a major policy shift: U.S. firms' crypto holdings become more observable in financial reports, but profit volatility also rises.

Chinese GAAP still lacks a dedicated standard. In practice most firms treat crypto as other current or non-current assets, test for impairment under prudence, and do not recognize unrealized gains. That produces inconsistent treatment across firms and hurts comparability of financial reports.

For Openverse participants, accounting choices must rest on a clear reading of the applicable standards: holding Bitgold as standby collateral—fixed asset, intangible, or financial asset? Holding Bitcurrency for operating settlement—cash or financial asset? Holding Bitsecurity as an equity investment—equity method or fair value? Each judgment needs confirmation with auditors and full disclosure in the notes, lest investors or regulators challenge the treatment.

Section 3. Identifying and Hedging Exchange-Rate Risk

Exchange-rate risk is the most basic financial risk for multi-currency firms, but in a crypto setting it covers a broader notion of “volatility between currency pairs” than traditional FX.

Traditional FX risk management distinguishes three exposures: transaction risk (future cash flows in foreign currency under signed contracts), translation risk (gains or losses when overseas subsidiaries' statements are converted into the parent' s reporting currency), and economic risk (the effect of FX moves on competitive position and long-run cash flows). The same three frames apply to crypto assets; only the pairs change—from “USD/EUR” to “USDC/Bitcurrency” or “Bitgold/USD.”

Crypto-to-fiat exchange rates (that is, fiat-denominated prices) are far more volatile than traditional FX. Bitcoin' s historical annualized volatility versus the dollar is roughly 60–80 percent, well above most major currency pairs (usually under 10 percent). Firms with large crypto holdings must set separate exposure caps and rebalancing discipline for high-volatility items; they cannot simply reuse FX practice designed for major pairs.

On hedges, traditional FX markets offer mature forwards, options, and swaps. Crypto hedge markets are developing quickly but still lag: liquidity depth is uneven (bitcoin options are relatively mature; small tokens have almost no derivatives); counterparty credit risk is far higher than at traditional banks (exchange failure risk was amply demonstrated by FTX); and tenor coverage is limited (long-dated hedges are costly and thin).

For crypto exposures that cannot be hedged effectively, common corporate strategies include: hard caps (crypto no more than X percent of total liquid assets); periodic rebalancing (when the crypto share exceeds the

target band, automatically convert the excess into fiat or stablecoins); and immediate liquidation after functional use (e.g., convert crypto receipts to fiat at once to shrink holding exposure).

Stablecoins (USDC, USDT, and the like) play a transitional role in this framework: relative to high-volatility crypto, they are a “temporary berth,” so funds are not over-exposed to price moves before settlement while remaining usable on-chain for the next step. If Bitcurrency maintains stability against its nominal peg unit, it will serve a similar function. Receivables and in-transit positions that linger in monetary form and never enter the next exchange structurally slow the operating cycle—liquidity management should serve sales and collection, not let positions recirculate on the books for their own sake.

Section 4. Operating Architecture for Multi-Currency Cash Management

For mid-sized and larger firms, multi-currency cash management needs a clear operating architecture, not only ad hoc case-by-case decisions.

Layered accounts and wallets are the foundation: tier one, fiat bank accounts (operating, reserve, and dedicated accounts segregated by business type); tier two, on-chain wallets (hot wallets for daily settlement, cold wallets for long-term reserves, multisig for large-value internal controls); tier three, protocol-layer holdings (PCIM collateral positions, DeFi liquidity, token lockups). Liquidity, risk, and authority differ by layer and require separate policies.

Cash-flow forecasting is the core challenge: the firm must forecast inflows and outflows in each currency, identify net exposures, and decide when to convert or hedge. Traditional ERP systems (SAP, Oracle, and the like) support multi-currency cash-flow forecasts but usually cannot read on-chain balances in real time. Firms need integration between chain data and ERP so that on-chain assets are visible in the finance system as they change.

Internal control is especially important in multi-currency, multi-chain settings. Private-key management is the heart of on-chain asset security—lost keys mean permanent loss; stolen keys mean immediate, nearly irreversible transfer. Multisig is best practice for enterprises: large operations require joint signatures from multiple internal authorizers, preventing single points of failure (compromised employees, internal fraud). Threshold signature schemes (TSS) and hardware security modules (HSMs) offer higher security grades for institutions with larger asset scales.

Timing of fund transfers is another operational difficulty. Bank wires typically clear T+1 to T+2; on-chain settlement on Ethereum mainnet is on the order of seconds to minutes. That gap demands precise settlement scheduling so that late funds do not trigger contract breaches or miss time-sensitive on-chain windows (e.g., topping up PCIM public-layer collateral, redemptions, or keeping VRC-12 security-layer positions clear of on-chain liquidation thresholds; VRC-10/11 parameters are in the glossary). Public currency suits open settlement; VRC-11 suits closed trade circles—finance leads must grasp the accounting and compliance meaning of both layers of positions.

Section 5. Tax Compliance: Multi-Dimensional Reporting Duties for Crypto Assets

Holding, trading, and using crypto assets create multi-dimensional tax duties across jurisdictions—one of the areas CFOs must plan earliest.

Capital gains tax: in most countries that classify crypto as an asset rather than money, gains on sale or conversion are taxable as capital gains (or corporate income tax, depending on the purpose of holding). Every sale must record historical cost, sale price, and holding period (which affects short- versus long-term rates) and

be aggregated in the annual return. High-frequency trading firms may face hundreds or thousands of lots; manual processing is error-prone and requires specialist crypto tax software (CoinTracker, TaxBit, and the like).

VAT and sales tax: paying for goods or services with crypto is often treated as barter, with the VAT base measured at the fiat equivalent. The economics match cash payment; only the taxable value must reference market price at the transaction moment, adding bookkeeping complexity. Some countries (e.g., the United Kingdom) exempt VAT on payments in “instrument-type” tokens such as bitcoin, but rules must be checked country by country.

Cross-border transfer pricing: transfers of crypto among entities of a multinational group must be priced at arm’s length and documented accordingly. Departures from market prices invite tax adjustments and back taxes. In volatile markets, compliant documentation of internal transfer prices is a continuing burden.

Information reporting: U.S. FinCEN requires FBAR for taxpayers holding foreign crypto accounts above \$10,000; FATCA requires foreign financial institutions to report accounts of U.S. persons, and some crypto exchanges are already in scope; the EU’s DAC8 brings crypto-asset service providers into automatic exchange of information and requires reporting of users’ crypto data to member-state tax authorities. These duties form a global compliance net; firms must assess applicability systematically.

Section 6. An Evaluation Framework for Bitgold as a Corporate Reserve Asset

CFOs considering Bitgold in the corporate asset mix need an evaluation framework, not a decision based only on affinity for the protocol design.

Start with liquidity. Book value is not enough; the firm needs the ability to monetize quickly at reasonable cost when required. How deep is the Bitgold market? What is average daily volume on major venues? Under stress (sharp market declines), how wide do spreads become? If the firm’s Bitgold holding exceeds about 10 percent of a venue’s average daily volume, its own liquidation will move the price and create significant market-impact costs.

Volatility and business correlation must be examined together. What is Bitgold’s historical price volatility? In extreme events (the May 2022 LUNA collapse and broader crypto drawdown, or the March 2020 liquidity crisis), how large were drawdowns? If Bitgold is held as PCIM/VRC-11 staking reserve, the firm must keep BTG buffered relative to the x^* threshold so that extreme markets do not force concentrated redemptions or top-ups (VRC-12’s security layer has separate on-chain liquidation thresholds; do not conflate them with PCIM/VRC-11). The correlation of Bitgold with the firm’s core cash flows also matters: crypto-industry service providers’ revenues track crypto market conditions closely, so Bitgold amplifies systemic risk; real-economy firms with low crypto correlation may have a coherent diversification rationale for a limited Bitgold reserve share.

Regulatory and reputational risk form the last filter. Crypto-holding firms must weigh pressure from regulators (auditors and compliance teams’ scrutiny of novel assets), banks (some may decline to bank crypto-holding clients for compliance reasons), and institutional investors (some ESG-oriented funds tilt against firms holding proof-of-work tokens). These non-financial factors are also decision variables.

Section 7. The CFO’s Strategic View: When and How to Enter the Multi-Currency Era

For most CFOs, the timing of multi-currency management should turn on whether real business needs have appeared and whether the organization can respond in an orderly way—not on whether a protocol whitepaper has been published.

Several real needs drive multi-currency demand: high-frequency cross-border payments where bank channels are slow and expensive; partners beginning to settle in crypto and requiring acceptance; entry into crypto-native ecosystems (Web3 service providers, on-chain protocol participants); and regulatory or tax arbitrage (jurisdictions where crypto is treated more favorably than fiat). Outside those scenes, multi-currency for its own sake only adds complexity without commercial logic.

When real demand appears, a sensible path is usually: begin with stablecoins (closest to fiat experience, clearer accounting); build wallets and internal controls before scaling (do not rush large on-chain operations before infrastructure is ready); fully understand the economics and technical risks before joining more complex protocols (such as PCIM staking); and retain accountants, counsel, and tax advisers who know crypto—do not rely on a single vendor’s judgment.

The whole entry process should be treated as capability building, not a one-off financial decision. Once multi-currency competence exists, it is infrastructure for digital-era financial management; without it, every new multi-currency scene starts from zero and costs accumulate. Treasury optimization must rest on continuing production and delivery—products must be made before markets open; liquidity management cannot replace supply-side creation.

Section 8. Crypto Asset Custody: Dual Architecture of Security and Compliance

Asset security is the first safeguard for corporate crypto holdings, and the security model differs fundamentally from traditional assets. Equities are protected by custodian banks, securities registries, and legal frameworks; ultimate control of crypto is the private key—once lost or stolen, assets cannot be recovered. Custody arrangements are therefore the link that most requires professional judgment.

Corporate crypto custody roughly follows three paths. Self-custody: the firm holds keys itself, with full control, and must build hardware wallets, multisig, and key-backup processes—suited to large firms with professional security teams. Institutional custody: assets go to licensed providers such as Coinbase Custody, Anchorage Digital, or BitGo, trading insurance and compliance reporting for custodian credit risk. Hybrid custody (MPC/TSS): multiparty computation or threshold signatures shard keys so that firm and custodian must authorize together, balancing autonomy and security.

Insurance is an important complement for large firms. Traditional property insurers do not cover crypto; a specialist market has grown in recent years, but coverage, pricing, and the number of carriers remain limited. Firms should work with insurance advisers to assess whether existing policies cover crypto and, where needed, buy dedicated cover so that even after a security incident losses stay within acceptable bounds.

Section 9. A Quantitative Framework for Cross-Currency Liquidity Management

Multi-currency liquidity management needs a quantitative framework, not only qualitative risk language. Currency exposure caps should map to board-approved risk policy—e.g., bitcoin no more than 5 percent of total liquid assets, stablecoins no more than 20 percent, Bitgold no more than 10 percent—not unilateral Treasury fiat. Liquidity coverage ratio (LCR) tests simulate the firm’s maximum funding need over thirty days under stress and check whether existing positions cover it under conservative haircuts (e.g., 70 percent liquidation discounts on crypto in extreme markets). Rebalancing thresholds balance transaction costs against drift risk—too frequent triggers generate tax events; too slow lets drift accumulate. Asset-correlation matrices under stress matter especially: in a systemic crypto decline, most crypto assets weaken together versus the dollar, so average correlations from normal markets overstate diversification benefits; the framework must include stress correlations.

Section 10. Rebuilding Organizational Capability in the Finance Function

Multi-currency management demands new organizational capabilities from finance. Traditional cores are fiat accounting, reporting, budgeting, and bank relationships. Crypto adds on-chain operations (wallet management, contract interaction), crypto risk assessment (volatility, liquidity, smart-contract risk), cross-border tax knowledge (multi-jurisdiction reporting), and collaboration with specialist crypto service providers.

Capability building usually follows three paths: internal training (blockchain, DeFi, and crypto accounting tools for existing teams—suited to well-resourced large firms); external hiring (finance talent with crypto backgrounds—suited to firms that must enter markets quickly, with attention to cultural fit); and outsourcing (custody, on-chain reporting, tax filing to specialists—suited to smaller firms for which build costs are too high, with oversight mechanisms required). Whatever the path, firms need clear accountability: who may authorize on-chain trades, who monitors risk parameters day to day, who decides in extremes, and how the audit committee obtains independent verification of on-chain operations. Clarity in that governance is the critical leap from “technically feasible” to “organizationally reliable” multi-currency management.

For firms considering the Openverse ecosystem, several non-financial incentives belong in the same decision frame as technical function and financial analysis: early participants often gain greater influence over standard-setting, parameter design, and governance proposals—growing from protocol users into rule-shapers. That “protocol equity” must be weighed against early technical risk, liquidity risk, and regulatory uncertainty; clear risk awareness and adequate capability preparation are necessary conditions for sustained operation in the multi-currency era.

注释与引用

1. FASB (2023), Accounting Standards Update No. 2023-08, *Intangibles—Goodwill and Other—Crypto Assets (Subtopic 350-60)*, §§4–6 (fair-value measurement; changes through earnings; effective for fiscal years beginning after 2025); by contrast IFRS still often follows IAS 38 historical-cost–impairment asymmetry for intangibles. <https://www.fasb.org/page/document?pdf=ASU+2023-08.pdf> ↩

§ 18 Supply Chain Finance and Private-Domain Settlement

Global supply chains move tens of trillions of dollars a year, yet still rely heavily on receivables, commercial paper, factoring, letters of credit, and other tools left over from the paper age—especially across borders, where information asymmetry, long confirmation cycles, and intermediary costs remain high. VRC-11 (Privcurrency) is built for stable settlement inside permissioned domains and fits bounded supply-chain networks by design. Whether on-chain protocols can rewrite supply-chain finance depends less on technology alone than on whether verification costs can be shifted forward—and whether core firms are willing to replace payment-term bargaining with auditable records.

Section 1. Traditional Pain Points in Supply Chain Finance

Electronics manufacturers such as Foxconn may stretch payment terms to upstream component suppliers to 90–120 days; SMEs then pledge receivables to banks, with annualized financing costs in emerging markets often above 15 percent. Platforms such as AntChain’s “Shuangliantong” and JPMorgan Onyx have piloted splitting core-firm credit into transferable on-chain credentials—limited in scale, but showing that private-domain settlement can substitute for part of bank factoring.

The core economic problem in supply-chain finance is timing mismatch. Manufacturers must advance raw-material purchases and production costs before buyer payment arrives, locking large volumes of receivables in transit. That mismatch is lethal for SMEs: big brands squeeze upstream suppliers with 60-, 90-, even 180-day terms, while suppliers’ working-capital buffers often cannot support such waits. Long terms split an exchange that should have completed in production into two halves: goods delivered, payment months later—liquidity stuck in non-productive waiting.

Traditional solutions include: receivables factoring (selling unmatured receivables at a discount for immediate liquidity); reverse factoring (core-firm-led, banks financing approved payables early to suppliers); bill discounting (acceptances exchanged for bank cash); and letters of credit (banks guaranteeing payment in import–export trade). These tools have centuries of legal framing and practice, yet share several structural limits.

Information asymmetry is the root problem. Before financing a supplier’s receivable, a financial institution must verify that the claim is real—trade occurred, goods delivered, buyer acknowledged. That process depends on manual review of paper documents (invoices, bills of lading, acceptance certificates), takes days to weeks, costs heavily, and still leaves room for fraudulent trade financing.

Multi-tier penetration is hard. Core firms (major brands) and tier-one suppliers have strong credit relationships, so banks willingly finance tier one. Tier-two and tier-three suppliers of raw materials often have no direct link to the core firm; institutions cannot verify trade background, and financing availability collapses. Supply-chain finance thus concentrates between large firms and tier one; SMEs’ funding distress is not systemically solved.

Cross-border scenes are more complex still. Receivables assignment rules differ across legal systems; enforcement of multi-country judgments is obstructed; FX volatility and divergent financial regulation raise friction far above domestic levels. Letters of credit, the classic cross-border payment guarantee, stack issuance fees, negotiation rates, and process time—especially uneconomic for small trades. Blaming payment gaps and financing shortfalls on “not enough money” often reverses cause and effect—the bottleneck is usually trade confirmation and credit assessment, not the supply of the medium of exchange itself.

Section 2. How Blockchain Rebuilds the Information Base Layer

Supply-chain finance's core obstacle is information; blockchain's core property is a shared, tamper-resistant record layer. That fit is where mainstream financial institutions and supply-chain firms most recognize blockchain's practical value.

On-chain trade documents: invoices, shipping notices, acceptance certificates, and related records go on-chain as multi-party, anytime-queryable electronic records. A buyer's on-chain signature confirming receipt is the most direct technical means for institutions to verify receivable authenticity—no manual paper review, no phone checks; contracts automatically inspect the buyer's on-chain confirmation state.

Smart contracts replace manual verification: in traditional factoring, institutions manually review documents, confirm claims, disburse, and monitor repayment. On-chain contracts can automate most of these steps: if the buyer has confirmed receipt on-chain and raised no dispute, the contract can trigger disbursement to the factor before the term falls due; at maturity, it can debit the buyer's on-chain account and repay principal and interest to the supplier. Friction costs and operational risk fall sharply.

Multi-tier penetration already has pilots: if an entire chain's trade records sit on one chain or interconnected private-domain chains, institutions can trace indirect links between tier-two/three suppliers and the core firm, assess real trade background, and extend financing to SMEs previously unreachable. Platforms such as PlatON, Trade Chain, and Bank of China's supply-chain finance systems have begun to pursue this.

Of course, on-chain records cannot automatically solve off-chain fraud. If goods never shipped but the chain shows delivery, blockchain only "upgrades" fraud into digital form. The authenticity link between physical logistics and on-chain records—IoT devices, third-party inspection, video verification—remains the weak joint in overall trustworthiness. On-chain records shift verification costs forward; they do not underwrite off-chain acceptance—fraud merely changes carrier.

IoT devices supply the most direct bridge between physical state and on-chain records: cold-chain temperature sensors upload transit status; RFID tags trigger on-chain entries at warehouse gates; GPS tracking provides continuous location streams. Integrated with smart contracts, these data can enable automated settlement—"pay when goods reach the designated place." Practice must face physical tampering or disconnection of devices, oracles as potential single points when data go on-chain, and uneven data standards across logistics firms that require industry-layer coordination. Until standards advance, hybrid approaches are often more feasible—critical nodes (loading, departure, arrival, receipt) authorized on-chain by humans, with automation only where data reliability is assured.

Section 3. Deployment Paths for VRC-11 in Supply Chain Finance

VRC-11 (Privcurrency)'s private-domain stablecoin character makes it naturally suited to supply-chain finance. A supply-chain network is by nature a bounded "private domain"—known identities, relatively stable trade relations, compliance requirements set in advance. That aligns closely with VRC-11's design for circulation on permissioned lists. Blueprint v2.0.0 uses an automotive chain as a template: the core OEM mints Privcurrency against Bitgold under the 61.8 percent undercollateralized rule (stake ratio 61.8 percent) and provides on-chain prepayment to parts suppliers; once delivery conditions are met, the contract automatically recovers financing principal and interest from subsequent payments—isomorphic to the Foxconn-style long-term structure in Section 1, but requiring verification of mainnet contracts and contractual enforceability in the relevant jurisdiction; the blueprint must not be treated as a production system already live¹.

In a concrete scene, VRC-11 deployment can be imagined as follows: a core brand, major suppliers, and cooperating financial institutions jointly enter a private-domain network settling in VRC-11. When trade occurs, the buyer issues a payment commitment (on-chain IOU) in VRC-11 to the seller; the seller may take that commitment to a network financial institution for early financing, which auto-assesses credit from on-chain state and disburses; at maturity, the buyer completes repayment on-chain and the institution recovers principal and interest. The bluepaper claims such arrangements can replace manual document checks in traditional factoring with “trade information on-chain in real time, tamper-resistant,” lowering institutions’ cost of assessing SME credit—but only if core firms are willing to put payables and logistics confirmations on-chain; on-chain tools must not become mere off-balance-sheet shadow channels.

In this flow VRC-11 serves two roles: settlement medium (the final unit of trade payment) and credit carrier (the on-chain payment commitment as the financing underlier). The closed private network ensures participants’ compliance status (KYC completed at onboarding), sharply cutting repeated verification costs in traditional factoring. If the network also admits VRC-10 public currency, the core firm can settle outbound procurement in Bitcurrency across borders and clear with tier-one suppliers inside the circle in enterprise Privcurrency (e.g., a brand’s StarUSD), forming a dual-layer Treasury—“public domain outside, private domain inside.” Peg-closure paths must be understood by layer: the VRC-10 public layer relies on current-tier overcollateralization (upper tier near 161.8%) + oracle same-price + mint/redeem arbitrage; the VRC-11 private layer relies on 61.8% undercollateralization + whitelist and off-chain redemption, with a structural gap $g(0) = 38.2\%$ from the first mint—not to be judged by public-domain $> 100\%$ standards.

Landing must clear three thresholds—technical, legal, and incentive. ERP must connect to on-chain contracts; document onboarding must automate, or manual inefficiency will cancel on-chain gains. Whether on-chain payment commitments have bill-equivalent legal force in each jurisdiction remains unsettled; institutions may refuse to lend on on-chain state alone. Whether core firms will put payment commitments and logistics confirmations on-chain depends on whether they will surrender the bargaining power that payment terms give them over suppliers—on-chain transparency is, for some, precisely a constraint.

Section 4. On-Chain Reconstruction of Factoring

Factoring is a core supply-chain finance tool: the supplier assigns unmatured receivables at a discount to a factor for immediate working capital; the factor collects from the buyer at maturity and earns the spread. Traditional factoring’s value is shifting liquidity risk from the supplier to a specialist institution and allocating risk through markets.

The basic on-chain vision: receivables tokenize, circulate and transfer in permissioned markets, and multiple factors bid, discovering optimal discount rates through competition. Traditional discounts come from a single factor’s quote; information asymmetry weakens suppliers’ bargaining power. On-chain bidding can introduce multiple quoters, compress financing costs through competition, and give suppliers fairer prices. Tokenizing receivables turns unmatured collections into transferable credentials—liquidity need not wait until the term ends.

On-chain factoring has unique advantages in small, high-frequency trade. Traditional factors usually set minimum ticket sizes; due diligence on small receivables costs too much relative to size, so SMEs struggle to get service. Automated on-chain verification sharply lowers per-ticket diligence cost, making small-ticket factoring economically feasible and potentially addressing long-tail SME financing availability.

A major obstacle today is legal recognition of receivables rights. In most common-law jurisdictions, assignment of receivables must meet specific formalities (e.g., written notice to the buyer) to bind third parties. Whether receivables interests represented by on-chain tokens meet those formalities differs by jurisdiction, and

many places have not yet clarified on-chain application. Completing the legal infrastructure for receivables tokenization is one institutional condition for scaling this track.

Section 5. Digitization and On-Chain Circulation of Commercial Paper

Commercial paper is another important traditional tool: firms issue paper or electronic acceptances promising to pay a stated amount on a stated date; holders may discount in secondary markets for immediate liquidity or hold to maturity for face value.

Putting bills on-chain is an important RWA (real-world asset tokenization) practice. Representing payment rights as on-chain tokens tradable among a wider investor circle may relieve thin liquidity in traditional bill markets—especially for SME-issued paper, which traditional markets discount heavily.

The core legal problem parallels on-chain receivables: paper bills have clear status and transfer rules under national negotiable-instruments law; electronic bills need special legislation (e.g., China’s Electronic Commercial Draft System, ECDS) to enjoy paper-equivalent force; fully on-chain bill tokens still lack clear status in most countries. That gap must be filled by legislation or judicial interpretation before on-chain bills can circulate without legal controversy.

China’s bill market has peculiarities. The PBOC-led ECDS is among the largest electronic-bill infrastructures, with daily turnover in the hundreds of billions of yuan. The incremental value of a distributed ledger atop this highly centralized system must be assessed carefully: if regulators do not open ECDS to on-chain protocols, distributed bill systems can only run outside ECDS, covering edge scenes the traditional electronic system does not reach—limited scale.

Section 6. Stablecoin Practice in Cross-Border Supply-Chain Settlement

Cross-border supply-chain settlement is among the most certain commercial-value scenes for stablecoins today. Using dollar stablecoins (USDC, USDT) for cross-border payment can compress traditional wire T+1–T+3 arrival to minutes and intermediary fees from tens or hundreds of dollars to near-zero on-chain gas. That efficiency edge is especially sharp in high-frequency, small-ticket cross-border payment (cross-border e-commerce, overseas payroll).

VRC-11 as Openverse’s private-domain stablecoin competes in this scene on differentiation versus mainstream stablecoins. USDC and USDT already have deep liquidity and broad exchange and merchant acceptance; if VRC-11 is “just another stablecoin,” network effects will be hard to win. Differentiation must rest on Openverse-specific scenes: if firms already using Openverse protocol suites for supply-chain management share VRC-11 as a natural settlement medium, adoption is an extension of protocol use rather than a separate adoption decision.

In practice, the main bottleneck in cross-border stablecoin settlement is often regulation and bank compliance, not the on-chain transfer itself. Most flows must still pass fiat on-ramp and off-ramp at some node—fiat to stablecoin, on-chain transfer, then back to fiat. Those steps go through regulated crypto dealers whose status differs sharply by country; in some emerging markets compliant channels barely exist. On-chain cross-border settlement most often sticks at this joint.

Section 7. Credit Layering and On-Chain Scoring in Supply Chain Finance

Traditional supply-chain finance assesses credit via core-firm endorsement (reverse factoring) or institution-by-institution diligence on single suppliers (forward factoring). Both paths have scale limits: how many suppliers a core firm will endorse is capped; so is institutional diligence capacity.

On-chain protocols offer a third path: dynamic credit scores from observable on-chain historical behavior. A supplier's two-year on-time delivery record, historical default rate, and stability of fund flows—if recorded on-chain—can automate much of credit assessment and extend coverage to long-tail SMEs institutions cannot diligence one by one.

Technical feasibility of this idea is already partly validated in traditional data dimensions (Alibaba Sesame Credit, WeChat Pay credit): algorithm scores backed by platform data have shown reasonable risk prediction in micro-lending. On-chain data's advantages are tamper-resistance and cross-institution shareability—traditional platform data are one platform's private asset; on-chain data are multi-party public assets; credit assessment need not depend on a single data provider.

The challenge is representativeness: if participants put only part of their business on-chain, records do not fully reflect true credit. If suppliers game scores by putting only good trades on-chain and handling bad ones off-chain, selective bias will distort the system. Reliability ultimately depends on completeness and credibility of on-chain data, secured through incentive design and multi-party verification.

Section 8. SME Financing Availability: Paths to Structural Improvement

The most important social value of on-chain supply-chain finance is structural improvement in SME financing availability. Globally, SMEs face a financing gap above \$5 trillion, acute in emerging markets. Traditional limits include: opaque financials (few audited reports, low data credibility); insufficient collateral (few fixed assets, hard to meet traditional loan requirements); high operating cost (diligence on a small loan costs nearly as much as on a large one); and weak bank relationships (little long-term history with institutions).

On-chain supply-chain finance can ease each of these, to varying degrees by scene. On-chain trade records are more real-time and harder to tamper with than audit reports; institutions can assess credit from trade behavior directly. On-chain-confirmed receivables themselves can serve as financing collateral, expanding SMEs' effective collateral set. Smart-contract automation lowers per-ticket processing cost, making small-ticket finance economic. On-chain credit scores can build files quickly from historical trade without prior bank relationships. Each verifiable on-chain delivery by a core firm opens financing headroom for upstream suppliers roughly equal to goods value—the financing gap is essentially temporary retention of value before final exchange completes.

These improvements have preliminary validation. China's "supply-chain finance + blockchain" products (AntChain's Shuangliantong, CCB's BCTrade, and others) have landed in manufacturing, agriculture, and other sectors, reaching tier-two and tier-three suppliers traditional finance could not cover. Cases prove the technical path is feasible and also reveal constraints: most successes depend on large core firms' push; if core firms will not drive the ecosystem on-chain, SMEs cannot digitize the whole chain alone.

Section 9. Agricultural Supply Chains: Among the Most Urgent Digitization Domains

Agricultural supply chains are among the most socially significant domains for on-chain supply-chain finance. Hundreds of millions of smallholders worldwide face severe financing difficulty: no fixed-asset collateral, exclusion from formal finance, dependence on high-interest loans for production funds—a vicious cycle of intergenerational poverty. If warehouse receipts, purchase contracts, and government subsidy proofs can tokenize on-chain, institutions can finance seasonal production against those credentials at costs far below traditional microloans.

The special challenge is the physical-digital link. Quantity and quality of produce must be confirmed by physical inspection or third-party certification; the credibility of putting those results on-chain depends on

inspectors’ integrity and anti-tamper mechanisms. IoT sensors (temperature/humidity, location tracking) can auto-upload some logistics data, but in remote agricultural settings deployment cost and reliability remain real constraints.

Even so, on-chain experiments in agricultural supply-chain finance are advancing in several emerging markets. Kenya’s Twiga Foods uses mobile data to track informal-market supply chains and extend credit to stallholders; India’s Jai Kisan scores farmers on agricultural data for unsecured loans; several Chinese agri-tech firms integrate subsidies, insurance, and loans on single digital platforms. Not all are direct applications of on-chain protocols, but they supply useful prior art on data foundations, business models, and compliance paths.

The intersection of agriculture and green supply chains offers an extra policy interface. Under Scope 3 pressure, firms must track emissions across the whole chain; if trade data are already on-chain, raw-material origin, transport mode, and process energy use can append on the same infrastructure into trade carbon-footprint records, with carbon credits circulating in permissioned networks. Low-carbon suppliers get better financing rates; high-carbon suppliers face higher costs—decarbonization incentives embedded in financing logic, not only administrative regulation. If VRC-11 takes on settlement in such closed trade circles, its value proposition exceeds ordinary B2B clearing; the direction remains early exploration and should not be treated as a proven business model.

Section 10. Phasing of On-Chain Adoption and SMEs

On-chaining supply-chain finance is a phased, scene-by-scene process, not an overnight replacement of bank intermediaries. In industries and regions with stronger digital foundations (core manufacturers in China, cross-border e-commerce supply chains in Southeast Asia), technology and business models are maturing quickly. Where legal infrastructure lags, technical capacity alone cannot drive scale.

Supply-chain finance may be the application of protocol money closest to the real economy: benefits often concentrate not on large institutions already in capital markets, but on SMEs excluded from traditional credit— instant settlement for cross-border micro-merchants, financing availability for tier-two and tier-three suppliers, payment-term pressure on manufacturing long tails. Long-run value of on-chain supply-chain finance projects should be judged by whether these groups’ funding conditions improve in substance, not only by large institutions’ reporting optimization.

注释与引用

1. Openverse Foundation, *VRC-11 Privcurrency Blueprint* v2.0.0, automotive-chain template (61.8% undercollateralization, on-chain prepayment and automatic recovery); source: official blueprint v2.0.0, not independently audited. https://cdn.openverse.network/docs/openverse_vrc11_privcurrency_blueprint_2.0.0.pdf ↩

§ 19 Tokenized Financing and Corporate Governance

Traditional equity financing depends on investment banks, exchanges, registrars, custodians, and other layered intermediaries; the barrier for SMEs to enter capital markets is extremely high. VRC-12 (Bitsecurity) lets firms stake Bitgold to issue equity-type tokens—a concrete realization of STO (Security Token Offering) logic inside Openverse. Whether tokenized financing and on-chain governance can ease traditional institutions’ chronic ailments must be tested objectively between ideal narrative and real constraints.

Section 1. Structural Predicaments of Traditional Equity Financing

Equity markets run on a precise intermediary ecology: investment banks (underwriting and pricing), stock exchanges (listing and matching), market makers (liquidity), securities registries (recording ownership), custodians (safekeeping), and auditors (verifying financial information). Each layer has a rationale—and fees and information control—that together form a significant barrier for SMEs.

In China, A-share IPO approval has long been known for strictness: from filing to approval typically takes two to four years; intermediary fees (underwriting, legal, audit) run from millions to tens of millions of yuan; disclosure is exhaustive, and any breach invites regulatory penalty. That has long created “shell value”—a listed company’s listing status itself is a scarce asset regardless of quality, spawning a distorted reverse-takeover market.

In the United States, small firms may raise from non-accredited investors under Regulation A+ (small public offerings) or Regulation CF (crowdfunding) with relatively lower regulatory thresholds, but liquidity is poor—these securities have almost no secondary market, and holders struggle to exit. The high liquidity of Nasdaq or NYSE listings comes at the price of stricter listing standards and ongoing disclosure duties.

Private markets (private equity, venture capital) partly fill the public-market gap, but participation thresholds (usually “accredited investor” status—high-net-worth individuals or institutions) exclude the vast majority of the public. Early equity gains of startups, in most countries, flow mainly to venture firms and their limited partners, not to public investors. Traditional equity financing’s layered intermediaries split issuance, pricing, and registration among separately licensed parties, each charging fees and holding information—making it harder still for SMEs to enter capital markets directly.

Tokenized financing attempts to break through these structural limits.

Section 2. The Issuance Logic of Security Tokens

A Security Token Offering (STO) represents and issues traditional securities interests (equity, debt, revenue rights) as blockchain tokens. The critical distinction from an ICO (Initial Coin Offering) is that an STO explicitly classifies the token as a security and voluntarily accepts securities regulation, rather than wrapping it as a “utility” or “instrument” token to evade securities law¹.

Potential STO advantages include: lower primary-market issuance cost (automated compliance checks and investor accreditation cut intermediary fees); better secondary liquidity (tokens on dedicated security-token venues can trade T+0 or even 24 hours, versus traditional T+2); global reach (tokens meeting specified jurisdictional requirements can, in principle, issue to global accredited investors, breaking the geographic limits of traditional IPOs); and smart-contract automation (dividends, buybacks, transfer restrictions handled by contract, cutting manual cost and friction). Financing must still map to verifiable cash flows or asset rights; if a

token is only a shell swap without anchoring underlying business, lively secondary liquidity will not support long-run pricing.

VRC-12 (Bitsecurity) operates inside this frame: firms stake Bitgold to issue Bitsecurity mapping equity or revenue-share ratios, trading on platforms with compliance whitelists. That is STO logic realized in the Openverse ecosystem. The Bitgold stake is a distinctive design—providing an extra value anchor (collateral value is non-zero, so the token has a floor of sorts) while introducing extra risk from Bitgold price volatility.

STO practice still faces significant obstacles. In the United States, Regulation D (private placement exemption) is the most common STO path, but holders must be accredited and face resale restrictions, blunting liquidity advantages. Regulation A+ allows issuance to non-accredited investors but caps offerings at \$12 million annually—unsuitable for large raises. Regulation S (offshore exemption) allows issuance to non-U.S. investors and is a common structure for cross-border STOs.

In the EU, MiCA supplies a unified crypto-asset framework but explicitly excludes security tokens, which remain under existing securities rules (e.g., ESMA’s MiFID II)—so compliance costs have not fallen materially. In Asia, Singapore (MAS’s “digital securities” framework) and Hong Kong (SFC’s security-token recognition regime) are relatively friendly jurisdictions with multiple live STO cases.

Section 3. Correspondence Between Equity Tokens and Traditional Shareholder Rights

Whether token holders truly possess “shareholder rights” is the legal question an STO must define most clearly. The token itself is an on-chain digital asset; holders’ rights over on-chain state are clear. Whether off-chain shareholder rights—voting, dividends, liquidation preference, information rights—fully map to token-holding status depends on the legal documentation at issuance.

A well-designed equity-token issue must build an explicit chain linking “token holding” to “legal shareholder rights.” Typical arrangements: a special-purpose vehicle (SPV) in the issuer’s jurisdiction holds the underlying equity; SPV beneficial interests map to token holders via lawful agreements; token balances in the smart contract serve as the on-chain basis for beneficial-interest ratios; SPV documents require the manager to distribute proceeds and transmit votes according to on-chain token records. If any link breaks—SPV liquidation, drafting gaps, inconsistency between on-chain and off-chain records—holders’ practical protection suffers.

On-chain voting is another critical mechanism. Traditional shareholders vote at annual meetings or by proxy; on-chain governance lets token holders vote proposals directly, recorded on-chain and unalterable by management. In principle that improves the classic dilemma of “small shareholders absent, proxies used by management.” Actual effect depends on several conditions: proposal content must be clear and comprehensible on-chain; vote outcomes must bind real corporate decisions (advisory-only votes are little better than performative democracy); and participation must be high enough to reflect diverse shareholder views.

Section 4. Reconstructing Disclosure On-Chain

Corporate-governance quality depends heavily on disclosure quality. Shareholders making informed decisions need timely, accurate, complete financial and operating information. Traditional listed-company disclosure relies on quarterly and annual reports (auditor-verified), ad hoc announcements (material events), and investor-relations activity (management outreach). The system’s problems: information flow is one-way (company to investors), and frequency is limited (information vacuums between quarterly reports).

On-chain protocols offer new infrastructure possibilities. If critical operating data—revenue, costs, cash balances, receivables status—can go on-chain via oracles in near real time, token holders can independently

check financial health at any moment rather than wait for quarterly reports. Smart contracts can be designed so that when cash falls below a threshold, holders receive automatic alerts; when material events trigger (e.g., large debt default), dividends pause and holder voting starts automatically.

This “continuous audit” vision is attractive, but difficulty should not be underestimated. Most corporate financial data live in centralized ERP; reliable on-chaining depends on oracle architecture, and oracles are among the most attackable weak points in on-chain systems. Financial-data authenticity has long rested on human auditor verification; automatic transmission from company-owned systems without independent verification is no more credible than unilateral management statements. Moreover, real-time publication of some financial data may harm competitive interests (live customer lists, order status); transparency and trade-secret protection must be balanced.

Even so, partial progress is feasible: balance changes in company on-chain accounts (financing round arrivals, large outflows) can be public in real time; token issuance and buyback records are fully transparent on-chain; on-chain records of major governance proposals and votes form a publicly inspectable decision history. Such partial transparency, even short of full real-time audit, is far faster and fuller than traditional semi-annual reports.

Section 5. Reconstructing Board Functions and the Boundaries of On-Chain Governance

The board is the core institution of corporate governance: entrusted by shareholders to supervise strategy, major decisions, and executive appointment. The traditional board is a small representative body—typically five to fifteen people—balancing multiple interests (large shareholders, independent directors, management) while preserving decision efficiency.

On-chain governance tools (DAO models) represent the opposite extreme: all token holders vote proposals directly, with no representative middle layer, fully decentralized decisions. That model has logic in fully decentralized open protocols (Uniswap, Compound)—no legal entity, no management, only protocol code and token holders. Transplanted directly to traditional companies, it meets a fundamental contradiction: a company is a legal subject that must perform contracts, pay taxes, and obey labor law; those duties need concrete persons and institutions, not waiting for token-holder votes before acting.

Hybrid governance is the more realistic path: the board retains strategy and day-to-day management; on-chain tools cover specific decision classes (holder votes on profit distribution, shareholder approval of major financings, consultation on long-term strategy); smart contracts execute automatable dividends, buybacks, and equity-record updates. The hybrid preserves legal-frame stability while introducing on-chain transparency and participation.

VRC-12 (Bitsecurity) issuers adopting this hybrid must draw clear lines in legal documents: which decisions go to on-chain votes, which to the board, which require both. Blurry boundaries produce power conflicts among governance organs and, at important decisions, no deterministic execution basis—raising legal risk for operations.

Section 6. Regulatory Contests and Global Practice in Token Financing

Since the 2017 ICO wave, global securities regulators’ stance on token financing has evolved from initial confusion toward active “substance over form” oversight. The U.S. SEC’s position is emblematic: if a token passes the Howey test (investment of money in a common enterprise with expectation of profits from others’ efforts), it is an investment-contract security subject to securities law. The SEC has brought multiple ICO enforcement actions seeking restitution and fines.

Against that backdrop, issuers who refuse to treat tokens as securities and claim “utility token” exemptions face high compliance risk—the SEC’s look-back authority means even years-old issues may later be pursued. More issuers therefore voluntarily accept securities classification and complete offerings through compliant STO paths.

Singapore’s framework is relatively STO-friendly. MAS’s 2020 digital-asset guidance makes clear that security tokens for public offering require a Capital Markets Services (CMS) license under the MAS framework. CMS-licensed issuers may offer security tokens to institutions and high-net-worth individuals along a relatively clear regulatory path.

Hong Kong SFC’s 2023 virtual-asset service provider (VASP) licensing regime and accompanying security-token recognition framework further consolidate Hong Kong as Asia’s compliant token-financing center. The SFC requires that security tokens offered to retail investors be SFC-recognized, with Chinese and English offering documents and disclosure oversight.

For mainland Chinese firms, both ICO and STO remain expressly prohibited. The 2017 PBOC and seven-ministry *Announcement on Preventing Risks of Token Issuance Financing* classifies token issuance as illegal public fundraising. Domestic firms needing token finance must build legal structures offshore (e.g., entities in Singapore or Hong Kong) and strictly segregate onshore business to avoid offering to onshore investors—operationally difficult and requiring specialist cross-border counsel.

Section 7. Exploring the Boundaries of DAOs as Organizational Forms

A decentralized autonomous organization (DAO) is the extreme form of tokenized governance: no traditional corporate structure; governance fully dispersed among token holders; protocol execution by smart contract. DAOs already have extensive practice in DeFi protocol governance, open-source funding, and investment clubs.

The core legal problem is subject identification: whose legal liability attaches to a DAO? If a DAO signs contracts, hires employees, or is sued, who bears liability? Under traditional law, DAOs lack legal personality, so all token holders may in theory face unlimited joint liability. That gap has been noted explicitly in several DAO-related suits.

Some jurisdictions have begun exploring DAO legal status. Wyoming’s 2021 DAO LLC statute—the world’s first—allows DAOs to register as LLCs with limited liability for token holders. The Marshall Islands, Cayman Islands, and other offshore centers are also developing DAO-adapted entity forms. These explorations supply institutional paths for DAO formalization, but also mean DAOs move from “fully decentralized, stateless organizations” toward “limited-liability entities bound by a specific jurisdiction’s law,” partly sacrificing the ideal of pure decentralization.

For most firms that need real commercial operations (not only protocol code), DAOs as the primary organizational form still face clear operational obstacles under current institutions. The hybrid path—a traditional legal entity as operating subject, DAO governance as the holder decision layer—is currently more feasible, and the structure VRC-12 Bitsecurity issuers are most likely to adopt.

Section 8. The Future of Token Governance: From Representation to Direct Democracy

The history of corporate governance runs from “ownership and management united,” through “ownership and management separated” (the birth of the modern corporation), to “refinement of ownership-level representation” (the rise of institutional investors and proxy voting). Tokenized governance supplies technical possibility for

evolution toward “more direct democracy”: more holders can participate in more decisions, not only attend an annual meeting and raise hands for management’s nominees.

But direct democracy is not naturally superior to representation. Voter short-termism (next-quarter profits over ten-year strategy), information asymmetry (individual investors understand strategy far less deeply than professional boards), and coordination failure (dispersed holders struggle to form coherent views, so organized voting blocs dominate important decisions)—these problems are well documented in political democracy and exist equally in corporate governance.

Tokenized governance’s contribution is to lower participation barriers, raise transparency, and widen accountability interfaces, not to replace professional boards. Holders can learn decision history at lower cost, express views on specific issues directly, and record voting positions on-chain—making information flows more symmetric and accountability more visible. On that basis, firms still need professional boards for high-quality strategic judgment; not every decision should be delegated to direct token-holder votes.

Section 9. Protecting Token Holders’ Rights: Why the Regulatory View Matters

Token-financing prosperity must not come at the systematic expense of holders’ rights. Historically, each rise of innovative financing tools (railroad bonds, internet stocks, MBS) has seen a boom followed by regulatory entry and investor-protection institutions. Token markets are in the middle-to-early stretch of that path: fraudulent projects, false disclosure, and insider manipulation remain serious problems.

Regulatory intervention is a double-edged sword: overly harsh rules choke legitimate innovation and push activity to regulatory-arbitrage venues; lack of protection exposes retail investors to systemic risk and damages public trust in the industry. Regulators worldwide are seeking dynamic balance between those poles; the overall direction is toward major securities frameworks—requiring token issuers to provide disclosure comparable to traditional securities offerings—while exploring token-specific rules (technical standards for automatic on-chain disclosure; smart-contract code audits as compliance requirements).

For issuers, voluntarily adopting disclosure above the regulatory floor is the most effective path to investor trust: independent auditors opining on issuance structure; regular on-chain reporting that transparently shows use of proceeds; holder complaint and dispute channels—arrangements beyond legal minimums that demonstrate attention to holder rights. Markets reward such issuers with trust premia: lower financing costs and more stable holder bases return the compliance investment.

Firms should select tools by business pain points first, then match compliance pace and risk tolerance—not chase narrative completeness in reverse. Cross-border settlement and private-domain supply-chain settlement already have commercial validation; tokenized equity and on-chain corporate governance remain early in the regulatory contest. Tokenized governance does not intend to overturn two centuries of company law; it probes, at the margins, more transparent rights transfer and wider participation interfaces—success or failure to be tested by markets and courts, not by narrative first.

Section 10. Lessons from Corporate Cases: Who Is Really Advancing Token Governance

Globally, those truly advancing tokenized financing and governance innovation are mostly crypto-native firms (exchanges, wallets, DeFi protocols—whose core business is on-chain finance, so token governance is a natural choice), tech startups (especially Web3, where token issuance solves financing and community building together), and traditional firms’ dedicated digital projects (e.g., large supply-chain platforms issuing asset-backed tokens under special-purpose structures). Full transformation of traditional industry champions into token governance remains rare.

Genuine cases of “traditional listed companies converting to token governance” are still scarce, and paths under current regulation are unclear. That suggests evolution of tokenized corporate governance is more likely “new firms built token-native from the start” than “existing traditional firms completing tokenized retrofit.” The strategic implication: traditional firms are better suited to “introduce on-chain tools to improve specific processes” (on-chain settlement for cross-border payments; on-chain supply-chain finance for financing availability) than to “migrate entire corporate governance onto an on-chain token frame.” Distinguishing those two goals—and avoiding radical decisions detached from own reality in pursuit of narrative completeness—is the judgment mature decision-makers most need in this transition.

Token financing markets are in a critical shift from early speculative experiment toward institutionalization: institutional investors (pensions, sovereign wealth funds, insurers) begin entering tokenized asset markets through compliant channels; specialist security-token venues obtain licenses; mainstream auditors offer dedicated audits for security-token issuers; judicial precedents on holder-rights protection gradually form. Institutionalization is both opportunity and constraint—depth and liquidity rise, compliance costs raise barriers, and many small issuers will be shut out. For VRC-12 (Bitsecurity), advance layout of regulated custody, institution-grade disclosure, target-market permissions, and investor-relations networks is required; these are market-entry costs, not deferrable afterthoughts.

Section 11. Triple Functions of Security Tokens and Regulatory Overlap

In the VRC asset lineage, VRC-12 (Bitsecurity) is classified as a security token—the third lineage besides public currency (VRC-10) and private-domain stablecoins (VRC-11)—and does not serve as a general medium of exchange or unit of account. On-chain security tokens compress three attributes that traditionally belong to different institutional links onto one programmable credential: equity (representing equity or RWA shares, carrying dividend claims), governance (on-chain votes on material matters), and circulation (transfer or pledge financing inside compliance whitelists). Functional synergy is real—shareholders can participate in governance, receive dividends, and collateralize tokens when needed—but regulatory classification must run on the securities axis, not as “money.”

That compound structure creates jurisdictional overlap: securities regulators focus on issuance disclosure and investor protection; company-law regulators on shareholder rights and board duties; AML and payments regulators may claim extended jurisdiction because of transferability—and the three sets of requirements are not always consistent. Bitsecurity’s design and compliance path should prioritize the STO frame under securities law, treating on-chain voting, dividends, and transfers as technical implementations of rights incidental to securities, not as a freestanding “money–security hybrid.” Payment scenes should settle in VRC-10/11; security tokens only represent equity transfer.

Resolving jurisdictional competition requires cross-regulator coordination in major markets or special legislation clarifying a unified frame for tokenized securities—long-term work at G20, FSB, and other multilateral layers. If Openverse is to operate lawfully in major global markets, it must join regulatory dialogue with securities compliance as the default path, offering auditable technical implementations rather than using a “monetary innovation” narrative to evade securities classification.

注释与引用

1. Arner, Buckley & Schularick (2022), "The Future of Stablecoins," *Journal of Financial Regulation* 8(2), pp. 155–179: security tokens must fall under traditional securities disclosure and investor-protection frames; Gorton & Zhang (2022), "Taming Wildcat Stablecoins," *University of Chicago Law Review* 89(1), pp. 1–52: systemic risk and regulatory paths for on-chain stable assets and security tokens. <https://doi.org/10.1093/jfr/fjac010> ; <https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins> ↩

Part VI: Value Networks for AI

§ 20 Silicon Networks and Participants in the Value Internet

Part V still centered human decision-makers: procurement signatures, board votes, bank-counter identity checks. When value-network nodes expand to APIs, sensors, and autonomous Agents, “who may spend, and under what rules” becomes a new question—they hold no passports, do not queue for accounts in business hours, yet already perform large coordination functions on the information Internet. When the Value Internet upgrades from “passing information” to “passing and settling value,” reputation updates on a quarterly clock while machine collaboration runs in milliseconds; whether constraint carriers can shift toward verifiable rules becomes a dimension monetary theory must take head-on.

Section 1. From the Information Internet to the Value Internet

Since the late twentieth century, TCP/IP, HTTP, SMTP, and related protocols have driven the cost of global information exchange near zero: an email can cross continents; a webpage can be fetched by any node; the sender need not care which OS or access provider the receiver uses. The information Internet’s success did not rest on one firm monopolizing all content, but on open protocols that let any node participate under a common syntax—precisely Mr. Hayek’s emphasis that “rules precede particular executors,” realized in engineering: protocols public, participants free to enter or exit, competition at the application layer, the routing layer not locked by licenses.

The Value Internet vision extends the same logic to settleable asset transfer. VTP (Value Transfer Protocol) is designed in Openverse documents as the value layer’s routing protocol: by analogy with email addressing and delivery, value messages can route across chains and asset standards in a unified format, without a custom bridge for every asset pair. At the theory layer one may also compare ISO 20022 financial messaging or HTTP-layer micropayment experiments such as x402 to grasp the general structure of “routing semantics separated from settlement semantics.” VTP does not replace each chain’s consensus and security model; it (if landed as designed) lowers the interoperability cost of “how value is addressed, identified, and delivered.” As HTTP only carries messages and does not vouch for content authenticity, VTP if landed owns the routing semantics of value messages; asset authenticity, issuance rules, and final settlement still depend on on-chain state and smart contracts.

The leap from information to value cannot be completed by adding a payment button to today’s Internet. Information can be copied with near-zero loss; value transfer must solve double-spending, finality, counterparty risk, and compliance identity. Information-Internet participants may browse anonymously; if Value-Internet participants cannot be identified or held accountable, large-scale commercial collaboration is hard to establish. Hence the Value Internet must, atop open-protocol spirit, add verifiable identity, auditable ledgers, and programmable settlement conditions—on-chain verifiable rules and public asset standards thus enter the discussion (protocol-neutral counterparts include already-running standards such as ERC/USDC). Permissioned private-domain stablecoins are already discussed in corporate supply-chain scenes; when the counterparty is a continuously running program rather than a legal person or natural person, whether that toolkit is more natural than fiat accounts must be tested by pilot data, not extrapolated from roadmaps.

Section 2. A Spectrum of Value-Network Participants

Entities in value networks may be roughly classed as carbon-based or silicon-based by “what decides.” Carbon-based participants include natural persons, companies, partnerships, nonprofits, and the like—legally identifiable, able to bear civil liability, open bank accounts, and sign legally recognized electronic signatures.

Silicon-based participants are system components without independent legal personality that nonetheless initiate economic acts automatically: API gateways that meter and bill, IoT sensors that collect environmental data and trigger contracts, trading bots that place orders by strategy, and large-language-model Agents that have rapidly entered public view—they receive goals, call tools, interact with other services, and complete multi-step operations without step-by-step human approval.

The division here is by institutional interface, not an ontological claim. A warehouse robot arm remains, in law, its owner's property; a SaaS platform's API remains, in contract, an extension of the operator's obligations. At runtime, however, what initiates payment requests, submits on-chain transactions, and consumes API quotas is often a program, not a human click. Traditional financial infrastructure assumes every payment rests on a traceable natural-person authorization chain: account opening requires in-person or video verification; large transfers require tokens or SMS codes; corporate payments require dual review by finance lead and cashier. Silicon subjects cannot satisfy those rituals at runtime—they have no "presence," no "self," and no "emergency counter" outside business hours.

Carbon and silicon nest together. Most silicon economic acts still require a carbon subject to bear ultimate off-chain responsibility: companies answer for erroneous payments by their automation; developers bear civil or criminal liability for contract vulnerabilities they deploy. The question is not whether silicon can fully escape carbon guardianship, but whether—when coordination frequency and grain rise to milliseconds, micropayments, and cross-service depth—requiring every value transfer to rewind to manual carbon authorization will kill at the start much collaboration that should occur. If the Value Internet is to carry a machine economy, it must offer silicon participants value interfaces matched to their runtime character—Agent wallets and machine-readable asset layers are concrete forms of that interface.

Section 3. Friction of Fiat Account Systems for Non-Human Subjects

Modern commercial-bank account systems are products of twentieth-century carbon society and paper identity. Opening an account requires valid ID, proof of address, face recognition or in-person verification; corporate opening requires business licenses, charters, legal-representative authorization, and beneficial-owner disclosure. Those requirements serve AML and KYC goals and are reasonable against natural-person fraud and shell-company laundering. Applied to "opening a settlement account for an inference-service instance deployed in a cloud region," however, they expose a structural mismatch.

The opening process mismatches silicon runtime from subject identification onward. Bank and payment-institution service agreements usually assume account holders are natural or legal persons, not "a service account in a Kubernetes namespace." Separate sub-accounts for automation in practice usually hang under the parent company's subject, with unified credit and reconciliation; the subsystem itself cannot own an independent, programmable off-chain balance view. Result: microservice A consumes B's API, yet ledger entries consolidate on the parent's general ledger; internal cost allocation depends on ex post ERP allocation rather than real-time value transfer.

Authorization likewise blocks automation. Online banking and payment APIs commonly require human-triggered second-factor authentication: SMS, tokens, biometrics. An autonomous Agent calling a paid data API at 3 a.m. on a market signal cannot wake the CFO for an SMS code. Some firms bypass real-time authorization with "prefunding + fixed API Key," but that moves credit risk forward into prepaid risk and cannot support fine per-call, per-volume, or per-second billing—contrary to the economics of cloud-native elastic scaling.

Business hours and clearing cadence form another friction layer. Interbank transfers are limited by central-bank clearing hours and holidays; cross-border wires pass correspondent chains measured in business days.

Silicon systems trade in seconds or milliseconds; fiat pipes' batch clearing differs by orders of magnitude. Firms often compromise with "end-of-day batch settlement," sacrificing timeliness in high-volatility scenes (compute bidding, on-chain arbitrage, real-time ad auctions) or concentrating risk on a few market makers.

Compliance-report grain closes the problem on the definition of "who." Regulation requires tracing "who paid whom for what"; in carbon scenes "who" maps to ID numbers or unified social credit codes. In silicon scenes "who" may be hundreds of concurrent instances under one legal person; traditional reports struggle to distinguish "the company" from "the company's automated agent No. 47." Without finer programmable identity and auditable logs, compliance departments often ban autonomous payment wholesale, and innovation stays in human-approval sandboxes. For money to perform its medium-of-circulation function, it sometimes must appear in its golden person—Marx put the requirement bluntly in Volume I of *Capital*¹; on-chain addresses and signatures, in silicon scenes, are the digital counterparts of that same function.

These frictions do not mean fiat systems should open exemption lanes for non-human subjects—money-laundering and fraud risks are real. They mean that, under equally strict auditability, on-chain accounts and smart contracts can supply parallel infrastructure: address as interface, signature as authorization, state as balance, twenty-four hours without interruption, each transfer bearing an immutable timestamp and call trail. The further question: should a firm's internal silicon components also hold on-chain positions constrained by governance rules?

Section 4. Silicon Coordination in the API Economy

The Application Programming Interface is the most visible form of the silicon economy. Maps, payments, SMS, model inference, logistics tracks—much modern commercial capability is sold as APIs per call or per month. Stripe, Twilio, AWS, and similar platforms build on the chain "developer registers → binds payment method → obtains API Key → program charges"; silicon appears to call, but the settlement node remains a carbon subject's pre-authorized card or account balance.

That indirect structure works at small scale; when the caller is itself automation and the call chain depth exceeds three layers, cost and liability attribution blur quickly. Example: Agent A calls Agent B's orchestrated "market research" skill, which in turn calls news and translation APIs. The month-end bill is one aggregated invoice; it cannot answer "which user query triggered which external API fee"—bad for internal pricing, Agent performance review, and abuse detection. Centralized platforms' "usage dashboards" are ex post statistics, not composable, verifiable settlement credentials.

On-chain micropayments and programmable limits offer another approach: each API call may accompany a tiny on-chain transfer or consume a verifiable "quota token." Caller address, callee address, timestamp, and parameter hash write to the same ledger; auditors, regulators, and partners can independently replay afterward without trusting a platform's unilateral CSV export. The economic counterpart paid for an API call remains a service as a special form of product; only the unit of measure shifts from invoice line items to on-chain events. Centralized API markets still have efficiency in cold start, customer support, and dispute handling; when on-chain settlement layers are widely adopted in pilots, metering and settlement may sink into protocol, decoupled from the application layer—as HTTP decoupled from webpage content—to be tested by x402 and similar pilot data, not whitepaper extrapolation.

Sensors and IoT form the other wing of the silicon economy. Smart meters, cold-chain probes, industrial machine-status reports—they do not produce "intent," yet produce data that can trigger economic consequences. If temperature exceeds limits, an insurance contract should pay; if equipment runs at full load, a bonus should pay the compute supplier per protocol. Realizing such logic with traditional bank accounts requires data

platforms to cloud, ERP to aggregate, and finance to initiate payment manually—delay measured in hours. After oracles feed data into smart contracts, payment can trigger in sync with data arrival—provided sensor identity, data signatures, and contract terms were lawfully configured by carbon subjects before deployment. The governance frame of silicon trigger / carbon liability continues the supply-chain lineage of “trade information on-chain, automatic debit at maturity,” only at finer subject grain.

Section 5. Agents as Emerging Economic Participants

The combination of large language models and tool-calling frameworks has moved “Agents” from academic concept into engineering reality. The user states a goal; the Agent decomposes subtasks, calls search, code execution, database queries, third-party payment, and other tools, approaching results over multi-turn interaction. Unlike fixed-rule RPA (robotic process automation), Agents’ action space is more open, so economic effects on the outside world are harder to enumerate *ex ante*: they may misread prompts, suffer prompt injection from malicious pages, or buy unnecessary services in the name of “completing the task.”

From a value-network view, Agents’ distinctiveness is that they combine silicon execution speed with the fuzzy boundary of carbon mandate. The user says “book me the cheapest flight”; the Agent may call comparison APIs, airline directs, even on-chain stablecoin payment—without step-by-step user confirmation. If the payment pipe remains a linked card account, risk sits with user and issuer; if the Agent holds an on-chain wallet, the risk structure becomes: who custodians the key, who sets spend caps, who recovers erroneous transfers. Agents already exceed “smarter scripts”: they are new participants on the Value Internet that may hold independent on-chain identity and balances; their institutional treatment will decide whether a machine-readable value layer can land.

Enterprise “employee Agents” and consumer “personal Agents” have different liability structures. The former run under employment contracts and information-security policy, with tool whitelists and spend policies set by the firm; the latter engage consumer protection, unauthorized debit disputes, and traditional financial-regulation issues. In either case, fully banning Agents from value transfer abandons automation’s efficiency dividend; fully unleashing them is unlimited risk. The middle path is “governed on-chain proxy accounts”: multisig, daily limits, pausability, auditability—on-chain-native capabilities that map precisely to control instruments fiat systems struggle to delegate cheaply to subroutines.

Section 6. VTP and the Lightweight Role of Value Routing

Clarify VTP’s place in the overall architecture first, lest stack layers blur. Openverse is designed as Layer 0—a global decentralized value-exchange layer: at the protocol layer it supplies value addressing, routing, final-settlement anchoring, and cross-domain interoperability, so that various Layer 1 networks (ecosystem app chains, Ethereum, Cosmos chains, consortium chains, and the like) can connect—not a closed Hub/Zone LAN. VTP, the exchange layer’s routing protocol, is intended to own format and delivery of cross-domain value messages; UNS (Universal Name Service) maps human-readable addresses to on-chain identifiers; VRC standards (VRC-10/11/12/20/721 and others) are designed to specify interface semantics for each token class—the layering above follows the Openverse whitepaper vision and still awaits mainnet and cross-domain interoperability tests. One envisaged value flow: a VRC-20 quota token on a Layer 1 app chain routes via VTP message to Layer 0 clearing anchors, then converts to VRC-10 Bitcurrency for cross-ecosystem payment; external Ethereum USDC may likewise enter the same exchange layer via VTP/bridges—in protocol-neutral terms, the same logic maps to “app-chain quota token → value-exchange-layer routing → stable settlement asset,” unbound to a single brand.

VTP does not answer “whether a token is trustworthy”—that is collateral ratios, issuer reputation, and regulation; it answers “how assets in different trust domains find one another.” For silicon participants that distinction is critical: when an Agent calls a contract, it must parse “whether the counterparty asset type is on the allowlist,” not “whether every hop on the whole routing path is honest.” In permissioned deployments, firms may confine VTP routing to their own consortium chains and audited public-chain bridges—drawing activity corridors for silicon employees.

Lightweight VTP access means: one need not dive into every routing-message field, but must grasp the economic meaning—the Value Internet is addressable and cross-domain like email, so silicon subjects can programmatically specify payees and asset types without maintaining a separate bank account and SWIFT code for every counterparty. The “multi-currency Treasury” the CFO faces becomes, at the silicon layer, “multi-asset-type positions”: stable settlement may prefer VRC-10/11 or already-live stables such as USDC/DAI; utility and points use VRC-20; permissions and device slots use VRC-721; time commitments use VRC-13—public/private domain, fungible/non-fungible, instant/term, chosen by counterparty and delivery tense.

Section 7. Boundaries of Carbon Guardianship and Silicon Autonomy

Fully autonomous silicon economic subjects that cannot be emergency-stopped by carbon subjects will not gain legal recognition in the foreseeable period. Regulatory trends worldwide strengthen rather than weaken ultimate beneficial-owner traceability. Hence the lawful path for silicon participation in value networks is almost necessarily limited autonomy under carbon guardianship: boards answer for automated Treasury strategies; individual users answer for Agent wallets they deploy; developers answer for smart contracts they publish.

Technical implementations of limited autonomy include: spend-policy contracts (transfers only to whitelist addresses), timelocks (large amounts delayed 24 hours, guardians may cancel), multisig thresholds (enterprise Agents require dual finance and ops signatures), and upgradeable proxy contracts (migrate to new logic on vulnerability discovery without losing historical audit trails). These mechanisms are already mature on-chain; the hard part is linkage to off-chain law—will courts treat “multisig refused a transfer” as the company’s true intent? Will regulators accept on-chain logs as AML reporting basis? Answers vary by jurisdiction and are evolving slowly.

In *The Denationalization of Money*, Mr. Hayek envisioned competing currencies that must win holders’ trust; for silicon participants, “trust” first appears as verifiable constraint: holders (or their guardians) can read the rules, predict worst-case loss, and assign liability after accidents. On-chain rules that are public and auditable fit that standard better than black-box API charging—but public is not the same as intelligible. Contract bugs, prompt attacks, and key leaks must be mitigated item by item with limits, whitelists, and guardian pause. Silicon participants will not overnight replace carbon subjects as centers of legal liability, but will add new node types to value networks; if money and asset protocols cannot serve those nodes, the machine economy will remain blocked outside fiat-account doors.

Section 8. The Settlement Debt Left by the Information Internet

Decades of “free” or “ad-subsidized” business models on the information Internet have masked costs that cross-organization settlement should have borne. Search, social, open-source distribution—marginal copy costs near zero—yet cross-firm API calls still often require manual commercial negotiation, annual contracts, and invoice reconciliation. When an Agent tries to auto-compose ten vendors’ capabilities for one task, ten different billing dashboards and ten different KYC thresholds form a barrier harder than technical integration. Commodity

circulation differs from one-shot barter: after value changes hands, the settlement chain must keep running—information-layer “free” precisely masks the fact that the value layer has not yet achieved continuous circulation.

The Value Internet will not replace that structure in the short run; it offers an optional settlement infrastructure: within circles willing to adopt on-chain standards, silicon subjects collaborate through unified asset interfaces; within circles still on fiat invoices, carbon subjects continue traditional flows. The two systems coexist long-term, linked by on-/off-ramps, corporate Treasury, and compliant custody—cross-border scenes often need the combination “on-chain speed + off-chain fiat landing.” Under coexistence pressure, where does increment more likely fall? For high-frequency, micro-amount, cross-domain, audit-needed machine-to-machine trades, on-chain protocols’ comparative advantage may amplify as instance counts rise—to be tested by pilot data, not whitepaper extrapolation; for low-frequency, large-ticket, heavily regulated human trades, fiat pipes remain the default for a long time.

Section 9. Verifiability: The Second Emergent Dimension of the Digital Age

In *Principles of Economics*, Menger argued that money emerges from barter rather than being decreed by legislation or contract in a single stroke: some goods, easier to divide, more portable, and demanded more widely, gain “saleability” advantages and are gradually accepted as a general medium of exchange. Saleability answers which physical properties make something more likely to take on monetary function—the first emergent dimension of classical monetary-origin theory. Chapter 6, Section 4 already operationalizes discipline on a global ledger as three layers of verifiable rules—execution–state–history²: execution verifiable (rules written into contracts then auto-execute), state verifiable (collateral ratios, balances, whitelists queryable in real time), history verifiable (transfer events permanently retained and replayable). This chapter elevates that three-layer structure to a digital-age second emergent dimension parallel to Menger’s “saleability”—verifiability: saleability governs liquidity and acceptance surface; verifiability governs whether rules can be independently rechecked by third parties (including programs). Silicon participants push the latter threshold to millisecond coordination, turning the “state layer” from institutions’ quarterly disclosure into programs’ real-time query.

For silicon participants, the book’s claim may be stated thus: when the participant set of value networks includes non-human economic subjects, the constraint unit of monetary competition must partly shift from “whether the issuer’s reputation is trustworthy” to “whether protocol rules can be independently inspected by any third party (including programs)” —Mr. Hayek wanted to change who issues notes; the silicon age must also change what constrains money. The proposition operationalizes on the three layers “execution–state–history”: N_1 rules publicly readable; N_2 execution and state independently inspectable; N_3 value units routable and exit-able; missing any condition, “popularization” degenerates into slogan or centralized packaging; silicon millisecond coordination amplifies missing N_2 into immediate counterparty risk rather than quarterly disputes that can be mediated afterward. The claim is protocol-neutral—unbound to Openverse or any single chain; USDC reserve attestation, DAI collateral-ratio on-chain queries, x402 facilitator receipts, ERC-4337 policy-contract state are different landings on the verifiability spectrum.

Reputation constraints update too slowly for millisecond M2M coordination; verifiable rules convert “discipline” from personal credit into protocol state independently recheckable by third parties (including programs). The shift is partial, not total: facilitator compliance, card-network KYC, and carbon guardianship remain reputation chains, but at the margin, whether silicon subjects can enter the default settlement set increasingly depends on whether rules are on-chain readable and history replayable.

Monetary emergence $\approx$ saleability ranking $\times$ verifiability threshold—the former from Menger’s dispersed selection over physical properties; the latter from three-layer verifiable rules of “execution–state–history.” Szabo

(2017) captures the same institutional need as “social scalability”: when participants need not know one another to collaborate, verifiable rules substitute for interpersonal trust costs—silicon Agents push that threshold to millisecond coordination³.

Emergent dimension	Menger / classical problem	Silicon-age problem	Operational definition	Typical observable metrics
Saleability	Ease of sale; breadth of demand	Liquidity depth; cross-counterparty acceptance	Divisibility, durability, breadth of demand	Daily volume, market-maker spreads, merchant adoption count
Verifiability	(Almost impossible to scale-test in the classical era)	Whether rules and state can be independently rechecked by programs	Execution / state / history three layers	Real-time readability of collateral ratios, T_{recover} , audit-script coverage

When an Agent calls ten APIs in milliseconds, counterparties cannot rely on “knowing the company’s CFO” to build trust; they must rely on independently recheckable constraints—whether collateral ratios meet stated levels, whether whitelists were tampered with, whether session-key quotas were exceeded. In Menger’s era, verifiability was limited by closed ledgers and human audit costs and could not scale into emergence mechanisms; global ledgers reduce it from institutional privilege to a public technical good—“rules over persons” in silicon scenes means precisely this.

If verifiability is indeed the second emergent dimension, then after controlling issuance scale and collateral volatility, stable assets whose collateral and reserve state are real-time auditable on-chain should show systematically shorter median time T_{recover} to restore peg after depegging than comparable stables whose reserves are only quarterly disclosed and not independently recheckable off-chain—USDC (auditable reserves) versus UST (algorithm not independently verifiable) in 2022–2025, and MakerDAO DAI liquidation data, can serve as preliminary test material⁴. Observable metrics include: T_{recover} (hours), purchasing-power deviation Δp in the 24 hours after a reputation shock, on-chain collateral-ratio query latency τ_{read} (seconds). If T_{recover} shows no significant difference, one should narrow “verifiability determinism” and instead test whether the reputation-shock transmission coefficient β_{rep} (peg deviation amplitude within 24h of issuer negative news) rises as reserve audibility falls.

Section 10. Institutional Experiments in Silicon Settlement, 2024–2026

Over 2024–2026, engineering experiments in silicon settlement have accumulated a set of comparable instances. Frontier schemes have mostly proved “whether automatic payment is possible”; debate has shifted to “whether the constraints payment rests on are verifiable”—x402 and AgentKit cover the former; agentic commerce and M2M/ISO standards still advance at the institutional-reputation layer; DePIN (Akash/Render/Bittensor and others) contests the latter boundary at the stake-slash layer. The tables below first give the Part VI core six-line comparison (main lines the book’s silicon theory must answer head-on); then summarize constraint-carrier differences by stack position; then attach the 2024–2026 frontier panorama. Openverse columns are labeled throughout; the same logic applies equally to ERC/USDC/x402 and the like. The “observable metrics” column gives quantifiable rebuttal metrics within 12–24 months—if measured results diverge from theoretical prediction, narrow rather than extrapolate conclusions.

Core six-line comparison (2024–2026, Part VI theoretical anchors)

Frontier main line	Core mechanism	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	12–24 month observable metrics
x402	HTTP 402 micropayments; Coinbase open-sourced 2025.05; x402 Foundation 2025.09	Reputation (facilitator)	Per-call settlement co-framed with HTTP; receipt replayable; policy hard for third parties to recheck	VTP messages + VRC-20 per-call quotas / VRC-10 stable settlement	Pilot success rate, γ_{gas}
AgentKit	CDP 2024.11; framework-agnostic on-chain action providers; integrates with x402	Reputation (custody)	Custodial-wallet layering; multisig/session keys partly on-chain readable	Contract wallets + UNS whitelist + VRC asset policy	Custodial mispay rate r_{mispay}
Agentic commerce	AP2/A2A (2025), Visa TAP, Mastercard Agent Pay, Stripe/Shopify Agent checkout	Reputation (card-network KYC)	Fiat M2M main path; authorization logs inside institutions; hard to replay on-chain	On-chain sub-ledgers + Privcurrency month-end reconciliation	Debit dispute rate, τ_{revoke}
DePIN / Akash	On-chain GPU/CPU order books; AKT stake bidding	Stake slash	Payment replayable; delivery proofs mostly off-chain	VRC-721 slots + VRC-10 stable settlement	SLA breach rate, order fill rate
DePIN / Render	RNDR settles by render job; output-hash acceptance	Stake + token incentives	Homogeneous tasks; volatile tokens poor as unit of account	VRC-11 private-domain compute pools + VRC-20 internal quotas	Share of acceptance disputes
DePIN / Bittensor	Subnet TAO stake and inference scoring markets	On-chain registration + slash	Sybil and volatile pricing risk	VRC-20 subnet quotas + soulbound reputation fields	Slash frequency, score-manipulation detection rate
M2M / ISO 20022	camt/pacs messaging; SWIFT CBPR+ global migration (2024–2025)	Reputation (clearinghouses)	Messages alterable off-chain; contrast with on-chain historical verifiability	VTP value-message semantics + on-chain receipt mapping	Message latency, reconciliation difference rate
M2M / IETF MPP	draft-ryan-httpauth-payment (HTTP 402 semantics standardization, 2025)	Reputation + device certificates	Condition-triggered payment; oracles as weak link	VRC-721 device keys + oracle price feeds	Condition-trigger false-positive rate

Silicon-settlement six-stack comparison (2024–2026)

Stack position	Representative scheme	Constraint carrier	Verifiability landing	Openverse	12–24 month observable metrics
HTTP micropayments	x402 (Coinbase 2025.05; x402 Foundation 2025.09)	Reputation	On-chain receipt replayable; policy on facilitator side	VTP messages + VRC-20 per-call quotas / VRC-10 stable settlement	Pilot success rate, γ_{gas}

Stack position	Representative scheme	Constraint carrier	Verifiability landing	Openverse	12–24 month observable metrics
Custodial wallets	Coinbase AgentKit (CDP 2024.11)	Reputation	Multisig/session keys partly on-chain readable	Contract wallets + UNS whitelist + VRC asset policy	Custodial mispay rate r_{mispay}
Card-network debit	Agentic commerce (AP2/A2A, Visa TAP, Mastercard Agent Pay, Stripe/Shopify)	Reputation	Authorization logs inside institutions	On-chain sub-ledgers + Privcurrency month-end reconciliation	Debit dispute rate, τ_{revoke}
DePIN compute	Akash / Render / Bittensor	Stake	Slash and order books on-chain inspectable; delivery mostly off-chain	VRC-721 slots + VRC-10/11 stable settlement	SLA breach rate, Δ_{deliver}
M2M messaging	ISO 20022 (camt/pacs), IETF MPP draft	Reputation	Messages alterable off-chain	VTP value-message semantics + on-chain receipt mapping	Message latency, reconciliation difference rate
Account abstraction	ERC-4337 (2023 mainnet; 2024–2025 Bundler ecosystem)	Parameters	Policy contracts, collateral ratios on-chain readable	Contract wallets + whitelist + PCIM collateral queries	Policy bypass rate, τ_{read}

2024–2026 frontier panorama comparison

Frontier scheme	Core mechanism (2024–2026)	Silicon participants	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	Observ metrics (2026)
x402	May 2025 Coinbase open-source release; September same year co-founded x402 Foundation with Cloudflare; revives HTTP 402; PAYMENT-REQUIRED / PAYMENT-SIGNATURE headers embed USDC and similar stable settlement; facilitator handles on-chain verification and delivery	API gateways, caller Agents	Payment protocol + facilitator reputation	Machine-readable settlement co-framed with HTTP calls; lacks multi-layer asset standards and stable-unit division of labor	VTP messages + VRC-20 quotas / VRC-10 per-call settlement	Pilot AI call set success gas as of call

Frontier scheme	Core mechanism (2024–2026)	Silicon participants	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	Observation metrics (2026)
Coinbase AgentKit	CDP release Nov 2024; framework-agnostic on-chain action providers (transfer, swap, contract calls); integrates with x402 for Agent autonomous payment	Deployer Agents	Platform reputation + API permissions + custodial signatures	Custodial-wallet layering; policy on platform side; hard for third parties to recheck independently	Contract wallets + UNS whitelist + VRC asset policy	Custodial Agent rate vs custodial multisig
ERC-4337 account abstraction	EIP-4337 (2023 mainnet); 2024–2025 Safe, Alchemy, Pimlico and other Bundler ecosystems; session keys, UserOperation batching	Contract-wallet Agents	On-chain policy contracts + multisig thresholds	Spend rules on-chain readable; Bundler is infrastructure, not reputation core	Contract wallets + whitelist + VRC asset policy	Policy-circumvent bypass upper limit on session leak loss
Agentic commerce / AP2	Google Agent Payments Protocol (AP2, 2025) and Agent-to-Agent (A2A) interoperability; Visa Trusted Agent Protocol (TAP, 2025 pilots); Mastercard Agent Pay (2025-04); Stripe Agentic Commerce API and Shopify Sidekick/Checkout Agent (2025–2026 pilots)	Agents as cardholders/shopping proxies	Card networks + bank KYC + platform reputation	Fiat M2M main path; weak on-chain replayable audit; constraint carrier still institutional reputation	On-chain sub-ledger records + month-end Privcurrency/fiat reconciliation	Debit denial rate; authorized revoke τ_{revoke}
DePIN / Akash	Decentralized cloud compute order books; AKT stake bidding for GPU/CPU	Buyer/seller Agents	Stake slash + order books	Compute order books; volatile token pricing; stable settlement needs layering	VRC-721 compute slots + VRC-10 settlement	Order fulfillment SLA breach rate
DePIN / Render	GPU render network; RNDR settles by render job	Render Agents, miners	Token incentives + output-hash acceptance	Homogeneous tasks; need stable internal unit of account	VRC-11 private-domain compute pools + VRC-20 internal quotas	Share of accepted hash data
DePIN / Bittensor	AI subnet TAO stake and inference markets	Multi-Agent subnet collaboration	On-chain registration + stake slash	Composable reputation; Sybil and volatile pricing risk	VRC-20 subnet quotas + soulbound reputation fields	Subnet event frequency score-risk

Frontier scheme	Core mechanism (2024–2026)	Silicon participants	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	Observ metrics (2026)
						manipu detecti
DePIN / io.net	DePIN market aggregating idle GPUs; IO token incentives	Compute buyer Agents, node operators	Stake + off-chain delivery proofs	Same class as Akash; delivery verifiability weaker than payment	VRC-721 slots + stable settlement layer	Node u vs actu comput delivery deviat
DePIN / Helium	HNT/IOT/MOBILE incentivize IoT/5G hotspots (2023–2025 network migrations)	Sensor gateways, coverage-proof nodes	PoC coverage proofs + oracle price feeds	Off-chain radio coverage hard to recheck independently	VRC-721 device slots + stable settlement	Hotspo uptime actual covera deviat
DePIN / Filecoin	FIL incentivizes decentralized storage; Proof-of-Replication	Storage buyer Agents, retrieval nodes	Spacetime proofs + stake slash	Storage delivery verification weaker off-chain than payment	VRC-721 storage slots + VRC-10 settlement	Storage rate; re latency
M2M / ISO 20022	Global payment messaging standard (camt/pacs series); SWIFT and national RTGS gradual migration	ERP, bank hosts, Treasury systems	Clearinghouses + institutional credit	Messages tamperable off-chain; contrast with on-chain historical verifiability	VTP value-message semantics	End-to-messag latency reconcili differ
M2M / ISO 20022 camt.054	2024–2025 multi-country RTGS and SWIFT gpi pilots enhance account reporting and reconciliation grain	Bank hosts, Treasury Agents	Clearinghouses + institutional credit	Messages alterable off-chain; fine-grain M2M reconciliation still depends on bank pipes	VTP messages + on-chain receipt mapping	Comple of cam chain t mappin
M2M / ISO 23485 draft	~~IoT device identity and payment triggers~~ → IETF MPP (draft-ryan-httpauth-payment, HTTP 402 semantics standardization; 2025); original ISO/NP 23485 was a consumer-IoT privacy draft (rejected 2018, not M2M payments)	Sensors, robots	Device certificates + bank pipes	Condition-triggered payment; oracles as weak link	VRC-721 device keys + oracle price feeds	Conditi trigger positive share c chain arbitra
M2M / ISO/IEC TR	Industrial IoT (IIoT) data exchange and	Industrial sensors, PLCs, AMRs	Device certificates +	Messages alterable off-	VTP messages + VRC-721 device	Device interop

Frontier scheme	Core mechanism (2024–2026)	Silicon participants	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	Observation metrics (2026)
30166	device interoperability reference architecture (2020–2024 revisions)		enterprise ERP pipes	chain; contrast with on-chain historical verifiability	slots	failure OT/IT reconciliation difference
M2M / GS1 EPCIS 2.0	Logistics event capture and sharing (2024 revision); Digital Link bridges device–message–payment triggers	Warehouse AMRs, cold-chain sensors	Event pipes + enterprise ERP	Events alterable off-chain; contrast with on-chain receipt replayability	VRC-721 device keys + oracle event hashes	Completeness of event payer mapping false-trace rate
Agent orchestration / MCP	Anthropic Model Context Protocol (spec 2024.11); OpenAI Agents SDK (2025); Google Agent2Agent (A2A, 2025) divided with AP2 payment-authorization chains —tool calling and settlement not yet a unified standard	Orchestration-layer Agents, skill plugins	Platform API permissions + custodial billing	Toolchains composable; settlement still platform reputation	VTP + VRC-20 per-call quotas + contract whitelists	Completeness of tool-payer mapping cross-platform reconciliation difference
x402 Paymaster networks	Coinbase CDP Paymaster and x402 facilitator networks (2025–2026 pilots); sponsor gas; aggregate USDC settlement	API gateways, caller Agents	Facilitator reputation + compliance review	Lower gas friction; policy and reserves still hard for third parties to recheck independently	VRC-10 per-call settlement + permissioned-domain facilitators	γ_{gas} decrease facilitator downtime
Cloudflare Workers × x402	Cloudflare (2025) integrates x402 payment headers in edge Workers; API per-call settlement co-framed with CDN calls	Edge APIs, caller Agents	Facilitator reputation + edge platform	HTTP micropayments + global edge; constraint still facilitator	VTP messages + VRC-20 per-call quotas	Edge payment success cold-start latency
Base L2 + CDP stack	Coinbase Base (2024–2026) hosts USDC, AgentKit, x402, and Paymaster combinations	Deployer Agents	Platform reputation + L2 sequencer	L2 lowers gas; sequencer and custody remain reputation layer	Layer 0 value exchange + VRC-10	L2 settlement latency sequencer downtime window
Solana Actions / Blinks	Solana Foundation (2024–2025); on-chain transactions embedded in URLs/QR	Consumer Agents, lightweight callers	Platform + RPC reputation	HTTP-layer trigger of on-chain settlement;	VTP messages + VRC-20 per-call quotas	Blink transaction success mispayment

Frontier scheme	Core mechanism (2024–2026)	Silicon participants	Constraint carrier	Protocol-neutral theoretical counterpart	Openverse design instance	Observ metrics (2026)
	codes; Blink API triggers swap/transfer			policy and reserves on RPC/wallet side		from R1 downtir
FedNow / RTP instant fiat	U.S. Federal Reserve FedNow (live 2023); UK FPS, EU SEPA Instant, and other 24x7 fiat instant pipes	Treasury Agents, ERP hosts	Clearinghouses + institutional credit	Fiat M2M main path; messages alterable off-chain; weak on-chain receipts	VTP messages + on-chain receipt mapping	End-to-latency reconc differe
PayPal Agent Checkout	PayPal (2025) Agent checkout integration pilots with OpenAI Agents SDK, Shopify, and others	Consumer Agents	Platform reputation + issuer KYC	Fiat debit main path; not independently replayable on-chain	On-chain sub-ledgers + month-end Privcurrency reconciliation	Debit d rate; τ_i
SWIFT gpi + ISO 20022	SWIFT gpi (2024–2025 enhancements); CBPR+ and camt/pacs global migration	Bank hosts, Treasury Agents	Clearinghouses + institutional credit	Messages trackable but alterable off-chain; contrast with on-chain historical verifiability	VTP value-message semantics + on-chain receipt mapping	gpi tra comple reconc differe
ERC-8004 Trustless Agents	Ethereum-ecosystem draft (2025); on-chain Agent registry + reputation/verification interfaces, combined with 4337 wallets	Multi-Agent collaboration, skill markets	On-chain registration + reputation fields	Composable reputation; Sybil and off-chain delivery still hard to recheck independently	VRC-20 subnet quotas + soulbound reputation fields	Registr share; reputat delivery deviatio

Most frontier schemes in the tables are at pilot or draft-standard stage; none alone proves that “the silicon economy has replaced fiat pipes.” Industry already treats non-human economic subjects as new nodes on payment networks; debate has shifted from “whether automatic payment is possible” to “whether the constraints payment rests on are verifiable.” x402 advances HTTP-layer micropayments to engineering usability; AgentKit sinks wallets and on-chain tools into the application layer; Anthropic MCP (2024.11) and Google A2A (2025) standardize Agent tool orchestration but have not yet closed settlement semantics—payment authorization still sits on reputation layers such as AP2/TAP; DePIN advances compute trading onto on-chain order books—constraint carriers for all four remain mainly platform reputation, facilitator compliance, or volatile-token incentives⁵. The differentiating claim of VRC design instances is to bring stable unit of account (10/11), quota layering (20), and permission slots (721) into one auditable standard family—an engineering proposal, not to be equated with already-running pilots such as x402.

At the theory layer, the six stack positions above map to three constraint-carrier classes: reputation (x402 facilitators, AgentKit custody, agentic-commerce card networks, M2M message pipes)—payment can occur; rules

hard for third parties to recheck independently; stake (DePIN slash, order-book deposits)—on-chain verifiable; off-chain delivery still weak; parameters (ERC-4337 policy contracts, PCIM collateral ratios, whitelists)—require on-chain state readability to become verifiable rules. The testable core of silicon monetary theory is: as M2M coordination frequency rises, marginal adoption of the parameter and stake layers relative to the reputation layer should rise—if 12–24 month pilot data do not support that, narrow “verifiability determinism” and instead test whether the reputation-shock transmission coefficient β_{rep} rises as reserve/policy auditability falls.

Participants in value networks are no longer only corporate and personal CFOs; they include APIs, sensors, Agents, and robots—programs and devices can likewise enter value transfer under public rules⁶.

注释与引用

1. Marx (1867), *Capital*, Vol. I, Ch. 3: “It functions as money ... when it has to be present in its own golden person. It is then the money-commodity.” Approximate Chinese sense: money is the money-commodity when it must appear in its golden person. Marxists English edition: <https://www.marxists.org/archive/marx/works/1867-c1/ch03.htm> ↩️²
2. Menger (1892), “On the Origin of Money,” §§1–2 (saleability); Chapter 6, Section 4, three-layer verifiable rules of “execution–state–history” (ch06 §4); Szabo (2017), “Money, Blockchains, and Social Scalability” (social scalability aligned with verifiability). <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↩️
3. Szabo (2017), “Money, Blockchains, and Social Scalability”: social scalability—participants need not know one another to collaborate; verifiable rules substitute for interpersonal trust costs; together with Menger’s “saleability” forms a two-dimension emergence frame. <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↩️
4. Viswanath-Natraj & Lyons (2023), *Journal of International Money and Finance* 131, 102777: dynamics of USDC re-peg after depegging; Lyons & Viswanath-Natraj (2020), NBER WP 27136: redemption arbitrage and peg-stability mechanisms; Coin Metrics (2024), *State of Stablecoins 2024*: UST 2022 depeg and DAI Black Thursday deviation benchmarks. ↩️
5. Anthropic (2024.11), Model Context Protocol Specification v2024-11-05 (JSON-RPC tool-call semantics; orchestration layer separated from settlement layer—MCP standardizes `tools/list/tools/call`, does not define payment receipts); Google (2025), Agent2Agent (A2A) Protocol Specification (Agent discovery, task delegation, and capability cards; complementary to AP2 payment-authorization chains); Ballandies et al. (2023), “A Taxonomy for Blockchain-based DePIN,” *Frontiers in Blockchain* 6, 1272380 (compute/storage/wireless DePIN taxonomy). <https://spec.modelcontextprotocol.io/specification/2024-11-05/> ; <https://github.com/google/A2A/blob/main/docs/specification.md> ; <https://doi.org/10.3389/fbloc.2023.1272380> ↩️
6. Coinbase (2025), x402 protocol specification and x402 Whitepaper (source: official whitepaper, not independently audited); Cloudflare & Coinbase (2025.09), x402 Foundation joint announcement; Cloudflare (2025), Workers x x402 integration docs (source: official docs, not independently audited); Coinbase Developer Platform (2024.11), AgentKit docs; Coinbase (2024–2026), Base L2 and CDP stack docs (source: official docs, not independently audited); Coinbase CDP (2025–2026), Paymaster and x402 facilitator network docs (source: official docs, not independently audited); Federal Reserve (2023–2025), FedNow Service docs; The Clearing House (2024–2025), RTP Network docs; PayPal (2025), Agent Checkout and OpenAI integration press (source: official press, not independently audited); SWIFT (2024–2025), gpi and ISO 20022 CBPR+ migration docs; Anthropic (2024.11), Model Context Protocol Specification v2024-11-05 (source: official protocol spec, not independently audited); OpenAI (2025), Agents SDK docs (source: official docs, not independently audited); Google (2025), Agent2Agent (A2A) Protocol Specification (source: official protocol docs, not independently audited); Solana Foundation (2024–2025), Solana Actions and Blinks docs (source: official docs, not independently audited); Ethereum Magicians (2025), ERC-8004 Trustless Agents discussion (draft, not mainnet-standardized); EIP-4337 (2023) account abstraction; Google (2025), Agent Payments Protocol (AP2) and Agent-to-Agent (A2A) specs (source: official protocol docs, not independently audited); Visa (2025), Trusted Agent Protocol (TAP) (RFC 9421 message signatures); Mastercard (2025-04-29), Agent Pay press (Agentic Tokens); Stripe (2025), Agentic Commerce API docs (source: official docs, not independently audited); Shopify (2025–2026), Sidekick / Checkout Agent pilots (source: official product docs, not independently audited); GS1 (2024), EPCIS 2.0 standard; ISO 20022 messaging standards; Render Network Whitepaper v4.0 (2017/2023, source: official

whitepaper, not independently audited); io.net Docs (2023–2025, source: official docs, not independently audited); Helium Foundation Docs (2023–2025, IoT/5G DePIN, source: official docs, not independently audited); Protocol Labs, *Filecoin: A Decentralized Storage Network* (2017/2022, source: official whitepaper, not independently audited); ISO/IEC TR 30166:2020 (IIoT reference architecture); Akash/Bittensor see Chapter 23 footnote ¹. <https://x402.org/> ; <https://www.x402.org/x402-whitepaper.pdf> ; <https://blog.cloudflare.com/x402/> ; <https://www.frb.services.org/financial-services/fednow> ; <https://www.theclearinghouse.org/payment-systems/rtp> ; <https://newsroom.paypal-corp.com/> ; <https://www.swift.com/our-solutions/swift-gpi> ; <https://spec.modelcontextprotocol.io/specification/2024-11-05/> ; <https://github.com/google/A2A/blob/main/docs/specification.md> ; <https://modelcontextprotocol.io/> ; <https://github.com/google-agentic-commerce/AP2> ; <https://developer.visa.com/capabilities/trusted-agent-protocol> ; <https://docs.stripe.com/agentic-commerce> ; <https://solana.com/developers/guides/getstarted/action> s ; <https://ethereum-magicians.org/t/erc-8004-trustless-agents/> ; <https://renderfoundation.com/whitepaper> ; <https://io.net/docs/> ; <https://docs.helium.com/> ; <https://filecoin.io/filecoin.pdf> ; <https://www.iso.org/standard/53211.html> ; <https://www.gs1.org/standards/epcis> ↩

§ 21 On-Chain Wallets and Micropayments for Agents

In 2024 Coinbase released AgentKit; in 2025 x402 bound HTTP requests to on-chain micropayments—autonomous programs in the fiat system still must open accounts, sign, and pass KYC. An on-chain wallet encodes “who may spend” as programmable signing authority, balance caps, and spending policies; payment shifts from “click to confirm” to the automatic execution of micropayments, streaming charges, and contractual splits.

Section 1 The Agent as Economic Subject

Traditional accounting and law assume that a “subject” is a natural or legal person. An Agent’s running instance is neither an independent legal person nor, in fact, merely idle: it initiates requests, consumes resources, and generates payables. Treating it as a pure tool means every act is immediately attributed to the deployer—simple but crude: one mistaken call may trigger tens of thousands of downstream API charges, and ex post attribution cannot restore the causal chain of each call. Treating it as a quasi-subject means giving the Agent a constrained on-chain identity: an independent address, an independent balance cap, an independent audit log. The deployer still bears ultimate responsibility, but internally one can distinguish “which Agent, which task, which outlay.”

In silicon-based settings the carrier of monetary discipline must shift in part from institutional reputation to verifiable rules. “Verifiability” stands alongside Menger’s “saleability” as a second dimension of monetary emergence—monetary emergence $\approx$ saleability ranking $\times$ verifiability threshold; silicon coordination pushes the latter threshold to the millisecond. Against frontier designs by three carriers—reputation, stake, and parameters: x402 and agentic commerce sit at the reputation layer; DePIN slash at the stake layer; ERC-4337 whitelists and PCIM collateral ratios at the parameter layer. The verifiability gradient of the three may be summarized as:

Constraint carrier	Typical schemes	What a third party can re-check	Weakness in silicon settings
Reputation	x402 facilitator, AgentKit custody, Visa TAP	On-chain receipts (partial)	Policy, reserves, and compliance sit with the institution
Stake	Akash / Render / Bittensor slash	Stake state, slash records	Off-chain delivery is hard to verify independently
Parameters	ERC-4337 policies, PCIM collateral ratios, whitelists	Contract state, collateral-ratio queries	Oracle inputs, governance capture

At the payment layer, whether an Agent enters the default settlement set depends, at the margin, more on whether spending policy, collateral state, and transaction history can be re-checked by a program than on whether a custodian’s brand is loud. The Agent wallet is the payment interface of this shift: reputational constraint rests on “trust that Stripe will not debit wrongly”; verifiable constraint rests on “any auditor can, at block height H, re-read transfer events and spending-policy bytecode.” The higher the frequency of silicon coordination, the greater the marginal value of the latter.

An on-chain address supplies a lightweight subject identifier. On Ethereum and compatible chains, an externally owned account (EOA) is controlled by a private key; a contract account is controlled by code. Agent practice commonly uses three modes: a custody service holds the EOA key and the Agent requests signatures via API; a smart-contract wallet (e.g. Safe multisig, ERC-4337 account abstraction) expresses spending rules in code—the Agent submits only an “intent,” and the contract decides whether to execute; a session key signs for the

main wallet within a limited time and amount and is revoked when the task ends. The three modes trade security against autonomy differently; there is no universally optimal solution, only a match to the business setting.

Another element of economic subjectivity is metering. The API economy already bills by call count, token count, and gigabyte-month of storage. Native on-chain metering can bind “consumption” to “payment”: when calling a data interface, the client simultaneously sends a stipulated quantity of VRC-20 quota tokens or a tiny amount of stable settlement asset to the server address (VRC-10 Bitcurrency for Openverse; protocol-neutral counterparts USDC/DAI); the server contract returns data after verifying receipt. The unit of account moves from a platform’s internal ledger to a verifiable on-chain event, laying the foundation for machine-to-machine (M2M) settlement.

Section 2 Machine-to-Machine Settlement (M2M)

M2M settlement means value transfer completed by programs under preset rules, without step-by-step human approval. “Automatic debit after goods receipt” in supply-chain finance is already an embryonic form of M2M, except that the subjects remain corporate legal persons. In the Agent era, M2M granularity can refine to a single inference, a single log retrieval, a single geocode—amounts that may fall below the minimum fee unit of traditional payment systems, producing the inversion “payment amount smaller than transaction cost.”

Since 2024, x402 (HTTP 402 micropayments), Coinbase AgentKit (on-chain tooling for Agents), and Visa/Mastercard agentic commerce pilots have approached the same problem from the Web-protocol layer, the custodial-wallet layer, and the card-network layer respectively: letting silicon subjects complete small settlements without stepwise human authorization. Anthropic’s Model Context Protocol (MCP, Nov 2024 specification) and Google’s Agent2Agent (A2A, 2025) standardize tool calls and task delegation at the orchestration layer—payment semantics still must be closed separately by AP2/x402 and the like¹. The core six-line comparison (x402, AgentKit, agentic commerce, DePIN three networks, M2M/ISO) is taken up below by M2M stack position with engineering detail.

x402 was open-sourced by Coinbase in May 2025; in September of the same year Coinbase and Cloudflare co-founded the x402 Foundation. The server returns HTTP 402 with a **PAYMENT-REQUIRED** header; the client Agent signs and retries with a **PAYMENT-SIGNATURE** header; a facilitator completes on-chain settlement in USDC or similar stables—payment and the HTTP call share a frame, but constraint still hangs on facilitator reputation and compliance review, not on independently re-checkable on-chain rules such as collateral ratios¹. AgentKit (CDP, Nov 2024) offers framework-agnostic on-chain action providers; integrated with x402, Agents can pay autonomously, but wallet custody reintroduces reputational constraint. The differentiating margin among the three is verifiability—whether each call can be independently replayed by a third party, and whether spending policy is on-chain readable. Against Openverse: VTP messages + VRC-20 per-call quotas + contract whitelists aim to embed x402’s “pay per request” in an auditable multi-layer asset standard; that combination is an engineering proposal, pending mainnet and compliance-interface measurement.

The table below summarizes mainstream schemes by M2M stack position, stressing differences in constraint carrier; the same logic holds for ERC-20/USDC; Openverse is listed as a design-instance contrast.

Stack position	Representative schemes (2024–2026)	Constraint carrier	Where verifiability lands	Protocol-neutral contrast	Openverse design instance	Observable metrics
Message / routing	ISO 20022, x402 (x402	Clearinghouse / HTTP payment	Off-chain messages mutable; x402	Financial messages vs	VTP value messages (interop	Message latency, reconciliation

Stack position	Representative schemes (2024–2026)	Constraint carrier	Where verifiability lands	Protocol-neutral contrast	Openverse design instance	Observable metrics
	Foundation, 2025.09)	headers + facilitator	on-chain receipts replayable, but policy sits with facilitator	on-chain event logs	pending verification)	discrepancy rate
Wallet / signing	AgentKit (2024.11 CDP)	Custodial reputation / contract state	Multisig thresholds, session-key quotas on-chain readable	Safe + session key	Contract wallet + UNS whitelist	Custodial mispay rate r_{mispay}
Account abstraction	ERC-4337 (2023 mainnet; 2024–2025 Bundler ecosystem)	On-chain policy contracts	UserOperation, session-key quotas on-chain readable	Policy written to contract state; Bundler not the reputational core	Contract wallet + whitelist + VRC asset policies	Policy-bypass rate, session-key loss upper bound
Card networks	Agentic commerce / AP2 / A2A / Visa TAP / Mastercard Agent Pay / Stripe Agentic Commerce / Shopify Checkout Agent	Card schemes + issuer KYC	Authorization logs inside institutions; third parties struggle to re-check independently	Fiat auto-debit as main path	On-chain sub-ledger + month-end Privcurrency reconciliation	Auto-debit dispute rate, τ_{revoke}
Agent orchestration	MCP (2024–2025), OpenAI Agents SDK (2025)	Platform API permissions + custodial billing	Toolchains composable; settlement still hangs on platform reputation	Orchestration layer separated from payment layer	VTP + VRC-20 per-call quotas	Tool-payment mapping completeness
IoT / M2M	IETF MPP draft, ISO/IEC TR 30166, GS1 EPCIS 2.0	Device certificates + bank/ERP pipes	Conditional triggers off-chain; chain records only results	Oracles as weak link	VRC-721 device keys + oracle price feeds	Conditional false-trigger rate
Compute / DePIN	Akash, Render, Bittensor, io.net	Stake slash + volatile tokens	Delivery proofs mostly off-chain; payments replayable	Slot NFTs + stable-settlement layering	VRC-721 slots + VRC-10/11	SLA breach rate, Δ_{deliver}
HTTP on-chain trigger	Solana Actions / Blinks (2024–2025)	Platform + RPC reputation	Blink receipts replayable; policy sits with RPC/wallet	URL-embedded swap/transfer	VTP + VRC-20 per-call quotas	Blink trigger success rate, RPC-outage mispay rate
Agent identity / reputation	ERC-8004 Trustless Agents (2025 draft)	On-chain registry + reputation fields	Registry queryable; off-chain delivery hard to re-check	Soulbound reputation + 4337 wallets	VRC-20 subnet quotas + soulbound fields	Sybil share, reputation-delivery gap

Stack position	Representative schemes (2024–2026)	Constraint carrier	Where verifiability lands	Protocol-neutral contrast	Openverse design instance	Observable metrics
Assets / pricing	USDC/DAI, VRC-10/11	Reserve audits / collateral parameters	balanceOf, collateral ratios queryable in real time	Auditable stablecoins	Bitcurrency / Privcurrency (pending mainnet test)	$T_{\text{recover}}, \tau_{\text{read}}$

On-chain micropayments try to break the amount inversion. Layer-2 rollups, state channels, and payment channels batch many small transfers to the main chain, spreading Gas cost; Openverse documentation layers a Layer 0 value-exchange layer and Layer 1 application chains—high-frequency business on Layer 1, final settlement and cross-domain routing anchored at Layer 0, to lower per-settlement friction—that layering must not be conflated with x402’s already-running HTTP micropayment pilots; together with x402 embedding payment at the HTTP layer and AgentKit wrapping signatures at the application layer, they occupy different stack positions of the same problem. Honesty requires acknowledging: micropayments may still be uneconomic when public chains congest; permissioned consortia or enterprise private chains are often more pragmatic in closed settings—private-domain VRC-11 settlement logic applies especially here. What M2M micropayments seek is to compress value exchange to the same frequency as silicon calls.

The credit model of M2M settlement differs from credit-card pre-authorization. On-chain settlement is usually “pay then service” or “atomic swap”: either payment and delivery complete in the same transaction (coupled by smart contract), or an escrow contract releases funds when conditions are met. The latter structure matters especially for Agents orchestrating complex service chains—user funds lock in the contract; sub-Agents claim shares by milestone, avoiding the chain risk of “upstream paid, downstream absconds.” Escrow and multisig are the default governance means for multi-Agent collaboration.

If the marginal advantage of on-chain M2M over x402/AgentKit is verifiability, then under the same API vendor and similar call volumes, firms using on-chain per-call settlement should show a lower per-call cost-attribution error rate ϵ_{attrib} (the share of month-end reconciliation that cannot be matched to a concrete Agent task) than firms relying only on centralized bills—measurable in 12–24 month pilots by “task ID $\leftrightarrow$ on-chain tx hash mapping completeness.” Observable metrics include ϵ_{attrib} , Gas as a share of call fees γ_{gas} , and custodial Agent mispay rate r_{mispay} (AgentKit-class controls). If ϵ_{attrib} shows no significant difference, the comparative advantage of on-chain M2M should be narrowed to compliance-audit settings, and claims of general efficiency gains should be withdrawn.

Testable proposition (frequency threshold): If constraint carriers migrate toward parameter/stake layers as M2M coordination frequency f rises, then after enterprise Agent call frequency exceeds a threshold f^* (e.g. daily mean $>10^4$ calls per API product line), the marginal adoption rate Δ_{adopt} of parameter-layer schemes (4337 policy contracts, PCIM collateral queries) relative to reputation-layer schemes (AgentKit custody, x402 facilitators) should rise—measurable in 12-month A/B pilots by stack-switch share. If Δ_{adopt} does not rise with f , the claim that “frequency drives constraint-carrier migration” should be narrowed, and one should instead test whether compliance cost κ_{audit} is the true driver.

Section 3 Custody, Multisig, and Spending Policy

When enterprises configure on-chain wallets for deployed Agents, they ordinarily should not hand the main Treasury private key directly to the program. A common architecture is layered: the main Treasury holds large reserves under human multisig; an operational hot wallet holds day-to-day liquidity with limited quota; each Agent

instance or Agent class holds a sub-account or sub-contract funded from the hot wallet by policy. Sub-account rules may encode: daily spend caps, per-transfer caps, transfers only to whitelisted contracts, no transfers to personal addresses, no calls to unaudited `approve` functions, and so on.

Multisig transforms “signing” from a biometric ritual into on-chain cryptographic consensus. Finance and operations each hold a key; abnormal Agent transfers cannot take effect unilaterally. This is akin to traditional dual-control bank–enterprise links, yet unbound by business hours, and the rules are publicly inspectable—internal audit and external supervisors can verify whether multisig policy has been tampered with, rather than trusting only a bank-issued PDF statement.

A smart-contract wallet’s “spending policy” may also include timelocks and pausable switches: when Agent behavior looks anomalous, a guardian can pause the sub-account in one click without waiting for bank support hours. By contrast, freezing a fiat account often requires judicial or regulatory process, with response times measured in days; on-chain pause is a self-rescue mechanism the deployer voluntarily embeds. Legal-effect boundaries still await case law, but engineering-wise it is already a standard requirement of enterprise secure operations.

Section 4 Micropayments and Streaming Payments

Micropayment means a single settlement of a tiny amount—typical scenes include per-call APIs, per-page content, per-second compute. Streaming payment releases continuously over time: e.g. transferring 0.001 dollars’ worth of tokens each second to a content provider; when the user stops consuming, payment stops, without prepaying a full monthly subscription. Combined, the two express a “pay for what you use” economic relation, close to the elastic usage essence of silicon systems.

Three main technical paths exist. State channels: parties exchange signed tickets off-chain and touch the chain only when opening or closing the channel—suited to high-frequency interaction with fixed counterparties. Sidechains or Layer 2: batch micro-transfers on a rollup and periodically anchor main-chain security. Direct on-chain micro-transfers: on networks with low enough fees, a simple transfer can stand—suited to permissioned or intra-enterprise chains.

In Agent orchestration, streaming payment can bind to “session lifetime”: the user opens a dialogue with an Agent and simultaneously opens a payment stream to the service provider; when the dialogue ends or times out, the stream closes automatically. This is fairer than “prepaid monthly membership” and more transparent than “ex post aggregated bills.” Implementation depends on wallet and front-end support for “streaming payment protocols”—Superfluid, Sablier, and similar Ethereum-ecosystem tools already supply precedents; Openverse documentation has envisioned folding similar semantics into VRC standards to reduce integration fragmentation; at the protocol-neutral layer one may also call existing Ethereum streaming contracts directly. Streaming payment splits “purchase” into continuous fragments synchronized with consumption, closer to elastic usage than monthly prepay.

Regulatory touchpoints of micropayments must not be ignored: large volumes of tiny cross-border transfers may be flagged by AML systems as structuring. Enterprises must set minimum retention records, counterparty whitelists, and suspicious-pattern alerts within a compliance frame—on-chain auditability here is an aid, not an exemption.

Section 5 Automatic Split via Smart Contract

When multiple Agents or multi-party services jointly complete one delivery, how is revenue shared? The traditional approach relies on ex post contracts and manual splits—high friction, many disputes. A smart

contract can, at the instant of receipt, split funds to multiple addresses by preset shares: platform cut 10%, data provider 30%, compute provider 40%, orchestrating Agent operator 20%—ratios written in code; the caller need not trust the platform’s honest ex post bookkeeping.

Automatic splits fit naturally with fungible tokens such as VRC-20: the receiving contract takes a stable settlement asset (VRC-10 Bitcurrency or VRC-11 Privcurrency as Openverse reference instances; protocol-neutral counterparts USDC/DAI or enterprise private-domain stables) and maps it by shares to beneficiaries; if a party must receive a specific utility token (e.g. API quota coin), the split logic can become multi-asset output. NFTs (VRC-721) may also participate: only addresses holding a specific capability credential may claim a share—used for “exclusive data sources” or “exclusive device time slots” and other non-fungible scenes.

For Agent platforms, automatic splits lower the trust cost of ecological cold-start: third-party skill developers are willing to integrate because on-chain rules guarantee a verifiable revenue share after each call, without fear that the platform will rewrite backend split ratios. The logic matches app stores and ad networks, but the execution layer sinks from the platform database to contract bytecode—the platform may still upgrade the contract, yet the upgrade itself must be public on-chain, and holders have a chance to exit.

Section 6 On-Chain Auditability and Centralized API Bills

Stripe, AWS, Azure, and other centralized platforms provide detailed usage bills and invoices—friendly to enterprise finance and meeting paper requirements for tax deduction. Their limit is that the bill is a unilaterally generated, theoretically mutable record; audit must trust the platform’s internal controls; cross-platform aggregation requires manual reconciliation; cost attribution fine-grained to “a single Agent call” often requires buying extra log-analytics products.

The core advantage of on-chain settlement is independent verifiability—“execution–state–history” here becomes “any auditor can replay transfer events at block height H.” x402 and AgentKit push “ability to pay” to engineering usability; whether a third party can independently re-check payment rules and state is the key discriminant of verifiable constraint at the M2M layer—AgentKit packages wallets, on-chain tools, and policy templates, yet constraint still hangs on custodian reputation; ERC-4337 session keys + whitelist contracts write constraint into queryable state, closer to “verifiable rules.” The UNS addressing + contract whitelists envisioned in the Openverse whitepaper point the same way in engineering instances—whether they beat AgentKit must await mispay-rate and audit-cost comparison at comparable scale, not design-document assertion. In an Agent economy, if each tool call accompanies an on-chain micropayment, task-level cost equals the sum of related transactions, without trusting the orchestration platform’s internal allocation algorithm; replayable on-chain transaction logs give silicon value circulation machine-readable physical evidence.

Centralized billing’s advantages should not be slighted either: customer support, refund disputes, credit-card chargebacks, VAT invoice issuance—these “soft services” that on-chain systems cannot natively cover remain a platform’s competitive edge. The realistic path is hybrid: on-chain records hard settlement facts; off-chain platforms issue fiat invoices from on-chain snapshots; or enterprises settle in private-domain chains with VRC-11 and make a one-shot fiat FX declaration at month-end. Dual-layer accounting—“silicon sub-ledger on-chain, legal-person general ledger off-chain”—is the natural extension of the CFO frame to this setting.

Auditability also changes abuse detection. Centralized platforms can ban malicious users internally, opaquely; in on-chain mode, anomalous spending patterns can be monitored by anyone (within privacy permissions), and communities and insurers can develop risk-scoring products. The cost is privacy: fully transparent micropayments expose commercial strategy and user behavior; zero-knowledge proofs and

permissioned chains become compromises—cryptographic detail is not pursued here; the tension between auditability and privacy will shape Agent-wallet product form.

Section 7 Risk One: Private Keys and Custody

The greatest technical risk of Agent wallets is private-key leakage. Humans can spot phishing mail; an Agent may read a private key from environment variables via a malicious page, a poisoned tool return, or a supply-chain-compromised dependency. Once leaked, on-chain assets are usually swept by automated scripts within minutes—unlike a credit card, one cannot call the bank to revoke.

Mitigations include: master keys never online, hot wallets with low balances, hardware security modules (HSM) or cloud KMS, contract wallets that restrict callable methods, and periodic rotation of session keys. Enterprises must bring Agent wallets under key-management procedures at the same tier as server certificates—many incidents stem from carrying “testnet key” habits into production.

Custodians offer compliance and insurance but reintroduce counterparty risk: users must trust the custodian not to misappropriate or be hacked. This resembles bank deposits, except that the regulatory frame is still immature. Self-custody retains cryptographic ownership but leaves operational risk entirely with the deployer. In Agent settings, pure self-custody is unrealistic for ordinary users; more feasible is “programmable custody”: the custody contract signs only when on-chain policy is met; the custody operator cannot see plaintext keys or move funds unilaterally.

Section 8 Risk Two: Prompt Injection and Rogue Tools

A distinctive risk of LLM Agents is prompt injection: attackers embed hidden instructions in web pages, mail, or database fields, inducing the Agent, while pursuing the user’s legitimate goal, to transfer funds, approve unlimited allowances, or sign malicious contract calls. Analogous to SQL injection, yet wired directly to the value layer—defense must cover input filtering, least-privilege tool permissions, and a hard rule that “value-transfer operations require human second confirmation.”

Rogue tools are forged APIs the Agent is induced to call: they return plausible data while routing funds to the attacker. Whitelisted tool registries, on-chain contract-address checks, and showing the user a “summary of the about-to-execute on-chain operation” are necessary engineering defenses. Fully autonomous Agent payment without human confirmation should exist only inside sandbox quotas with a clearly bounded loss upper limit.

“Autonomous Agent steals coins” is often painted in media as science-fiction catastrophe; the more common reality is misconfiguration and social engineering: developers hard-code keys into repositories, users grant Agents excessive permissions, phishing sites mimic wallet connect. Regulatory response may require that “autonomous payment” bind to a real-name subject and traceable logs, rather than a blanket ban—parallel to “substance over form” in token-fundraising regulation.

Section 9 Session Keys, Account Abstraction, and UNS Addressing

ERC-4337 account abstraction further decouples “signing authority” from “asset custody”: users or enterprises deploy smart-contract accounts; an EntryPoint contract validates UserOperations; Bundlers batch them on-chain. For Agents, spending rules become upgradeable policy modules—e.g. “auto-execute only when the call comes from a registered Agent-service IP range and the amount is below a threshold”—without waking human multisig each time.

Session keys are a lightweight variant of account abstraction: the main wallet authorizes a temporary key to sign within a limited time window, limited contract methods, and limited cumulative quota. After an Agent finishes

one “research task,” the session key expires automatically; even if leaked, the main Treasury is not at risk. The logic resembles a credit card’s “single-use virtual number,” yet is enforced by an on-chain state machine without issuer human intervention.

UNS (Universal Name Service) addresses readable naming in Agent orchestration. Silicon subjects programming payments prefer transferring to addresses resolved from human-readable names rather than memorizing forty-two-character hex strings. Openverse documentation maps readable names to on-chain identifiers via UNS and links them to VTP routing messages—when configuring tool whitelists, an Agent may declare “pay Privcurrency only to addresses under permitted domains,” lowering mis-transfer risk. The protocol-neutral counterpart is ENS and similar on-chain name services; supply-chain private networks already name Privcurrency with enterprise brand prefixes (e.g. StarUSD); UNS extends the same naming logic to the cross-domain routing layer.

In deployment practice, enterprises should build a “policy template library” per Agent class: customer-service Agents allow only micro VRC-20 quota consumption; procurement Agents may pay VRC-11 to whitelisted supplier addresses (permissioned domain); R&D Agents may call external model APIs but require multisig approval for Bitcurrency outlays above a threshold (public-domain stable settlement). Templates map one-to-one to on-chain contracts; at audit one can compare “policy document” with “on-chain bytecode” directly—verifiability that traditional online-banking USB-key permission tables rarely provide.

Section 10 Fiat On-Ramps, Off-Ramps, and Dual-Track Accounting

Agent on-chain wallets and fiat accounts will coexist for a long time: wages, rent, and taxes still require fiat; on-chain micropayments suit machine-to-machine, intra-ecosystem, and programmable scenes. On/off-ramps, stablecoin mint/redeem, and banks’ cooperation with judicial freezes of on-chain flows form the transition layer between the two systems.

At deployment, enterprises should write on-chain wallet uses into dual-track compliance and engineering files: allow API settlement, forbid speculative trading; allow Privcurrency in-circle payment, forbid large transfers to non-KYC addresses—and execute against smart-contract whitelists, shrinking the crack between compliance and engineering.

On/off-ramps remain the bottleneck of silicon wallets. Compliant exchanges converting fiat to on-chain Bitcurrency or enterprise Privcurrency must complete KYC and source-of-funds review; the Agent itself cannot perform that ritual—a carbon-based guardian must complete it before deployment and set periodic fiat top-up rules for the hot wallet. At month-end reconciliation, on-chain micropayment flows can export as CSV mapped to ERP accounts—“silicon sub-ledger on-chain, legal-person general ledger off-chain” dual accounting requires CFO and engineering jointly to maintain the chart-of-accounts map, rather than treating the on-chain wallet as a simple substitute for a fiat account.

Dispute handling and chargeback have no native on-chain equivalent. Credit-card chargebacks protect consumers when the merchant fails to perform; on-chain transfers, once confirmed, are usually irreversible. Agent commerce therefore relies more on ex ante escrow, reputation deposits, and pausable contracts than on ex post bank mediation. If a platform offers users “Agent payment protection,” it must build off-chain reserves and arbitration rules and make clear in the UI the difference from on-chain irreversibility—lest users assume holding Bitcurrency enjoys the same protection as bank deposits.

Section 11 Engineering Deployment and Asset Selection

Enterprises deploying Agent on-chain wallets should start from a minimum viable configuration rather than stacking every module at once: a separate sub-account or session key per Agent class; spending policy written into auditable contracts; VRC asset whitelists and UNS resolution; fiat top-up cadence and month-end reconciliation—tool calls involving value transfer must require human second confirmation or a loss-capped sandbox; if any link is missing, the pilot may still start, but known risk should be logged. The wallet answers “who may spend, and how”; the machine-readable value layer must also clarify asset types—VRC-20 carries fungible utility, VRC-10/11 public- and private-domain stable settlement, VRC-721 permissions and slots, VRC-13 time commitments, chosen by counterparty domain, delivery tense, and scarcity. Agents’ default settlement path does not go through VRC-12 (Bitsecurity)—security tokens represent equity flow and require a securities-compliance frame; they are unfit as machine micropayment or everyday unit of account. Openverse instance parameters follow public documentation.

注释与引用

1. Coinbase (2025), “x402: HTTP-native micropayments” protocol specification and x402 Foundation joint announcement (2025.09; source: official protocol docs, not independently audited); Coinbase Developer Platform (2024.11), “AgentKit” documentation (source: official docs, not independently audited); Anthropic (2024.11), Model Context Protocol Specification v2024-11-05 (source: official protocol specification, not independently audited); Google (2025), Agent2Agent (A2A) Protocol Specification (source: official protocol docs, not independently audited); OpenAI (2025), Agents SDK documentation; Solana Foundation (2024–2025), Solana Actions and Blinks documentation (source: official docs, not independently audited); Ethereum Magicians (2025), ERC-8004 Trustless Agents discussion thread (draft); Google (2025), Agent Payments Protocol (AP2); Visa (2025), Trusted Agent Protocol (TAP); Mastercard (2025-04-29), Agent Pay press release; Stripe (2025), Agentic Commerce API; Shopify (2025–2026), Checkout Agent pilot; IETF draft-ryan-httpauth-payment (Machine Payments Protocol); ISO/IEC TR 30166:2020; EIP-4337 (2023) account abstraction; Ballandies et al. (2023), DePIN taxonomy. <https://x402.org/> ; <https://docs.cdp.coinbase.com/agentkit/docs/welcome> ; <https://spec.modelcontextprotocol.io/specification/2024-11-05/> ; <https://github.com/google/A2A/blob/main/docs/specification.md> ; <https://github.com/google-agentic-commerce/AP2> ; <https://developer.visa.com/capabilities/trusted-agent-protocol> ; <https://solana.com/developers/guides/getstarted/actions> ; <https://ethereum-magicians.org/t/erc-8004-trustless-agents/> ; <https://doi.org/10.3389/fbloc.2023.1272380> ↩ ↩²

§ 22 The Machine-Readable Value Layer

Humans read bank SMS and invoices; programs read contract return values and event logs. If on-chain assets follow public standards (the VRC family, the ERC family), a program can query balances, authorize transfers, and trigger splits without parsing PDFs—that is the machine-readable value layer. Operationalization of verifiability is in Chapter 6, Section 4 (the three layers of execution–state–history).

Section 1 From Human-Readable Bills to Machine-Readable Interfaces

Traditional value representation relies on human-readable media: bank SMS, paper invoices, numbers on an ERP screen. If silicon coordination still needs OCR or web scraping to learn a balance, friction will cancel the gains from automation. Machine-readability requires that value state be exposed in a deterministic syntax: given an address and a block height, any node returns the same balance; given a transfer function and parameters, any node can predict the state-transition result.

The core contribution of blockchain token standards is precisely to harden that readability into an interface specification. ERC-20 defines methods such as `balanceOf`, `transfer`, and `approve` for fungible tokens on Ethereum; any compatible wallet, exchange, or DeFi protocol can integrate without discrimination. The VRC series functionally parallels and extends the ERC family; if Layer 0 value-exchange + Layer 1 application-chain layering is delivered, asset types on the value internet may still keep composable semantics when accessed across chains and across Layer 1s. VTP (if delivered as designed) is intended to handle message routing at Layer 0, while VRC specifies “what kind of value the message carries”—a division of labor analogous to TCP/IP and HTTP.

The machine-readable interface is the operationalization of verifiability’ s second emergence dimension at the asset layer. Chapter 6, Section 4 decomposes verifiable rules into three layers—execution–state–history¹; Menger’ s “saleability” decides whether an asset can be widely accepted as a medium of exchange; verifiability decides whether a program can independently re-check issuance rules and balance state at millisecond scale—in silicon settings the latter is often tighter than the former. $\text{Monetary emergence} \approx \text{saleability ranking} \times \text{verifiability threshold}$ —the former from Menger’ s dispersed selection over material properties; the latter from three-layer verifiable rules.

Mapping of the three layers onto asset interfaces: execution verifiable—transfer/approve execute by bytecode; state verifiable—`balanceOf`, collateral ratios, and whitelists queryable in real time; history verifiable—transfer events permanently retained and replayable. In Menger’ s era verifiability was limited by closed ledgers; a global ledger reduces it from an institutional privilege to a public technical good.

“Machine-readable” does not contradict human-readable. Block explorers and wallet UIs can render the same state as graphics; the difference is that silicon subjects can call the interface directly, without bank portals and business hours designed for carbon-based users. Public value interfaces lower the integration threshold for new participants (including Agent developers), yet they do not automatically guarantee asset quality—poorly collateralized “stablecoins” and infinitely minted points are, technically, also “standard interfaces.”

Section 2 Fungible Tokens: ERC-20 and VRC-20

A fungible token is an on-chain asset each unit of which is interchangeable, without individual serial differences. Ethereum’ s ERC-20 is the de facto standard; VRC-20 is intended to offer a parallel interface for points, API call quotas, game vouchers, governance votes, general utility coins, and similar scenes—functionally

equivalent to ERC-20; if Layer 0 / Layer 1 layering is delivered, deployment on a Layer 1 application chain must follow local gas and naming conventions.

Typical Agent uses of VRC-20 include: API quota coins—an enterprise issues `COMPANY_API_CREDIT`; each internal microservice call consumes one or one-tenth of a unit; insufficient balance fails the call without real-time fiat settlement; ecosystem points—users earn points for tasks, redeemable for services or discounts, with on-chain verification against double-spending; general utility coins—as an intermediate exchange unit in open Agent markets, reducing the complexity of N^2 bilateral pricing among N services.

Reasons to choose VRC-20 rather than fiat stablecoins directly are often boundary and incentive: quota coins can be minted without bound inside a private domain without shocking public monetary supply; points can set expiry and non-transfer rules (via contract constraints), whereas stablecoins usually must remain transferable to keep monetary properties. Regulatorily, if VRC-20 is widely used for external payment and pegged to fiat value, it may touch e-money or payment licensing; if confined to a closed ecosystem as a utility credential, the compliance path is closer to prepaid cards or loyalty programs—analysis must be jurisdiction-specific, not one-size-fits-all.

On integration, an Agent completes a micropayment by calling `transfer` or `transferFrom` (after prior `approve`); batch airdrops, mining rewards, and splits all speak the same interface. Developers must mind integer precision and `decimals` configuration to avoid floating-point error causing contract revert.

Section 3 Stable Settlement: VRC-10 and VRC-11

High-frequency Agent collaboration must answer “in what unit to price and settle.” Volatile speculative tokens are unfit as everyday units of account; public- and private-domain stable settlement assets therefore become the machine economy’s default choice.

PCIM public layer (Openverse instance: VRC-10 Bitcurrency) competitively issues against volatile collateral (Bitgold) with dynamic-tier overcollateralization (circulation-tier referenda; upper tier about 161.8%), representing ISO 4217 fiat units on-chain and serving as unit of account and medium of final settlement—these parameters come from the Openverse whitepaper, without independent audit or long mainnet testing; mechanism-neutral counterparts include DAI (ETH overcollateralized CDP), USDC (fiat reserves), and other auditable stable assets. For Agents, public Bitcurrency fits: cross-enterprise, cross-ecosystem scenes that must be roughly comparable to external fiat—paying public DApps, buying on-chain public data, or exiting to fiat via off-ramps. Its public nature means unified rules and network-wide liquidity aims, but also broader regulatory attention and collateral-parameter risk.

VRC-11 Privcurrency is an enterprise or permissioned trade-circle private stablecoin, designed in the blue paper to mint against Bitgold at low collateral (stake ratio 61.8%), circulating inside a permissioned whitelist, often named with a brand prefix (e.g. StarUSD, MicroUSD)—stressing scene binding rather than a rigid dollar peg; protocol-neutral counterparts are enterprise stables or internal settlement tokens on permissioned chains. Supply-chain scenes have already discussed deployment paths; in Agent scenes, Privcurrency fits: M2M settlement within one legal person or alliance, internal API markets, and B2B collaboration that prefers not to expose all flows on a public explorer. Agent wallets on permissioned domains or consortium chains may consider Privcurrency as the default unit, with month-end fiat aggregation declared at the CFO layer.

The relation of the two is “public outside, private inside,” consistent with enterprise Treasury multi-currency configuration across public/private domains. Agents should not be hard-coded to “recognize only one coin”; the orchestration layer must dynamically choose VRC-10 or VRC-11 by counterparty domain, amount, and compliance

need, converting via DEX or protocol-native swap when necessary—and conversion itself should be a machine-readable standard operation.

Section 4 Non-Fungible Assets: NFTs and VRC-721

Each non-fungible token (NFT) has a unique identifier and is not interchangeable. Ethereum's standard is ERC-721; Openverse's counterpart is VRC-721. Human narrative often links NFTs to art collecting; in the machine economy, more practical uses are permissions, slots, and device keys.

Permissions: only addresses holding a specific `tokenId` may call an API or a smart-contract method—an on-chain capability credential. The Agent must first verify that its wallet holds a valid VRC-721, then initiate the request; the server contract simultaneously checks `ownerOf`.

Slots: scarce resources such as compute markets, warehouse units, and spectrum time slots can be represented as exclusive rights by `tokenId`. Booking a GPU slot means transferring or staking the corresponding NFT; when the slot ends, VRC-13 time logic or a contract timelock releases it automatically.

Device keys: IoT device identity and operating rights can bind to VRC-721; only Agents holding the key NFT may send on-chain commands to the device, reducing unauthorized remote-control risk.

NFTs are unfit as everyday micropayment media—poor liquidity, high pricing friction. Agent scenes should follow the division “settle with fungible stables, authorize with non-fungible credentials.” If an NFT is both collectible and access card, secondary-market speculation may disturb operational stability: permission NFTs should be non-transferable or only permissioned-transferable, lest critical device keys flow into speculative markets.

Section 5 The Time Dimension: VRC-13 Light Link

VRC-13 (Time Token) tokenizes professional service hours, project deadlines, and service commitments; individuals may also issue service credentials backed by their own time. In Agent scenes, time tokens fit time-bounded use rights rather than permanent permissions: e.g. “one hour of consulting daily for the next thirty days,” “a data subscription valid this quarter.”

Openverse official docs also list VRC-30 (Timing Token) defining validity windows by block height; the text below keeps VRC-13 wording—when consulting the whitepaper, note the numbering correspondence with VRC-30. For Agent orchestration, time tokens may combine with VRC-721: 721 means “which slot,” 13 means “when that slot is valid.” The smart contract checks time-token state at `block.timestamp` or an agreed block height and rejects service calls when expired.

Time tokens should not be treated by Agents as general means of payment—they are non-fungible, time-bound, and often indivisible. The selection principle: when the value core is “a service commitment over a period” rather than “a good delivered instantly,” introduce VRC-13; when the value core is “instant settlement,” use VRC-10/11 or VRC-20.

Section 6 Four Asset Classes for Agent Scenes: A Comparison

The table summarizes standard positioning and selection principles for four asset classes in Agent orchestration. “Four classes” means stable settlement (VRC-10/11), fungible utility (VRC-20), non-fungible permission (VRC-721), and time commitment (VRC-13)—stable settlement lists one public and one private example, compared jointly on decision dimensions.

Asset type	Standard	Typical uses	Agent selection principle	Main risks
Public stable settlement	VRC-10 Bitcurrency	Cross-ecosystem payment, public DApps, on-chain unit before fiat exit	Counterparty in public domain; need fiat-comparable value; flows publicly auditable	Collateral-parameter and regulatory-policy change
Private stable settlement	VRC-11 Privcurrency	Alliance M2M, supply-chain circles, internal API markets	Counterparty on permissioned whitelist; need to isolate external flows; align with CFO private Treasury	Whitelist governance and stake-ratio maintenance
Fungible utility	VRC-20 (parallel to ERC-20)	API quotas, points, governance votes, ecosystem intermediate coin	Need divisible micro-amounts, high-frequency transfers, programmable incentives	Compliance boundary if deemed payment instrument or security
Non-fungible permission	VRC-721 (parallel to NFT)	API rights, device keys, resource slots	Need unique ID, non-interchangeable, often with timelock	Secondary-market ops interference; loss means loss of rights
Time commitment	VRC-13 Time Token	Subscription windows, professional service hours, time-limited votes	Value consumes with time or expires	Performance disputes need off-chain arbitration

Decide first whether the counterparty is in a permissioned domain—if yes, prefer VRC-11; else VRC-10; then whether payment is instant delivery or continuing rights—instant uses stables or VRC-20 quotas; continuing rights consider VRC-13 and VRC-721; unique slots issue VRC-721; divisible points alone suffice with VRC-20.

Section 7 On-Chain Assets as Value Interfaces

Synthesizing the standards above, on-chain assets are machine-readable, contract-callable value interfaces, not mere speculative tickers. Interface meaning includes: queryable (`balanceOf`, `ownerOf`), transferable (`transfer`), authorizable (`approve/setApprovalForAll`), composable (DeFi-style nested calls), auditable (event logs permanently retained). Agent developers call these interfaces as they call REST APIs; the difference is only that state changes require signatures and cannot be unilaterally revoked.

Silicon subjects do not “trust” an issuer’s verbal promise; they verify that interface behavior matches deployment (unless the contract is upgraded—and upgrades themselves should be visible on-chain). x402’s pay-per-call solves “how to trigger payment”; VRC/ERC standards solve “what is paid and whether rules can be independently re-checked”—both layers must hold for the machine economy to scale. The table below summarizes 2024–2026 experiments and VRC design division by asset-layer role:

Frontier layer	Representative schemes	Constraint type	Settlement-asset form	Verifiability gap	VRC design division
HTTP micropayments	x402 (2025.05; x402 Foundation 2025.09)	Reputation	Per-call USDC / facilitator settlement	Missing stable pricing layers; collateral ratios not independently re-checkable	VRC-20 per-call quotas + VRC-10 stable settlement
Paymaster	x402 Paymaster / CDP facilitator (2025–2026 pilots)	Reputation	Sponsored Gas + USDC aggregation	Facilitator reserves and policy hard for third parties to re-check	VRC-10 per-call settlement + permissioned-domain facilitator

Frontier layer	Representative schemes	Constraint type	Settlement-asset form	Verifiability gap	VRC design division
Agent toolkit	AgentKit (2024.11 CDP)	Reputation	Multi-asset in custodial wallet	Policy on platform side; third parties hard to re-check	Contract wallet + whitelist + UNS
Agent orchestration	MCP (2024–2025), OpenAI Agents SDK (2025)	Reputation	Platform custodial bills	Toolchains composable; settlement not standardized	VTP + VRC-20 per-call quotas
Account abstraction	ERC-4337 (2023 mainnet; 2024–2025 Bundler ecosystem)	Parameters	Multi-asset contract wallet	Bundler downtime not reputational core; policy must be on-chain readable	Contract wallet + whitelist + VRC asset policies
Card-network auto-debit	Agentic commerce / AP2 / A2A / Visa TAP / Mastercard Agent Pay / Stripe / Shopify	Reputation	Fiat authorization	Not independently replayable on-chain	On-chain sub-ledger + Privcurrency month-end reconciliation
M2M messaging	ISO 20022 / IETF MPP draft / ISO/IEC TR 30166 / GS1 EPCIS 2.0	Reputation	Bank/ERP pipe settlement	Messages mutable off-chain; conditional triggers hard to re-check	VTP message semantics + VRC-721 device keys
DePIN compute	Akash / Render / io.net / Bittensor	Stake	Volatile tokens + slot NFTs	Delivery proofs off-chain; pricing volatile	VRC-721 slots + VRC-10/11 accounting
HTTP on-chain trigger	Solana Actions / Blinks (2024–2025)	Reputation	URL-embedded swap/transfer	RPC/wallet policy hard for third parties to re-check	VTP + VRC-20 per-call quotas
Agent identity	ERC-8004 Trustless Agents (2025 draft)	Stake/reputation	Soulbound reputation fields	Off-chain delivery hard to re-check independently	VRC-20 subnet quotas + soulbound fields
Instant fiat M2M	FedNow / RTP / SEPA Instant (2023–2025)	Reputation	24x7 fiat instant; messages off-chain	Weak on-chain receipt	VTP messages + on-chain receipt mapping
Platform Agent checkout	PayPal Agent Checkout (2025 pilot)	Reputation	Fiat auto-debit; not replayable on-chain	On-chain sub-ledger + Privcurrency month-end reconciliation	

Three constraint carriers—**reputation** (platforms, facilitators, card schemes, RPC), **stake** (DePIN slash, order books, Agent registration deposits), **parameters** (collateral ratios, whitelists, session-key quotas)—each have weaknesses in silicon settings: reputation is hard for third parties to re-check independently; stake struggles to cover off-chain delivery; parameters become verifiable rules only when on-chain state is readable. x402’ s on-chain receipt partly reinforces reputational constraint; ERC-4337 policy contracts write spending rules into queryable state; VRC-10/PCIM collateral queries and 721 slots try to decouple DePIN’ s “programmable markets” from a stable pricing layer. Choosing asset standards is, in substance, allocating the verifiability burden between parameter and reputation layers.

Observable implication (colinear with P-22): If parameter-layer asset standards are indeed silicon's comparative advantage, then before and after the same DePIN vendor is integrated, an Agent scheduler's ρ_{audit} (reconciliation/audit scripts as a share of integration engineer-hours) should fall, and τ_{read} (collateral-ratio/whitelist query latency, seconds) should be below the dispute-mediation latency τ_{revoke} of reputation-layer schemes—comparable in a 12-month dual-track pilot.

Public value interfaces lower machine-economy integration cost but do not automatically guarantee asset quality. Poorly collateralized “stablecoins,” infinitely minted points, and admin-revocable NFT permissions are technically also “standard interfaces”—markets and regulators must screen. Monetary popularization expands the space for trial and combination; risk does not vanish.

If the core gain of a machine-readable value layer is verifiability, then after an Agent orchestration system adopts a new asset standard, the share of integration hours spent on “reconciliation/audit scripts” ρ_{audit} should fall while the share on “business logic” rises—comparable in dual-track projects where the same team integrates ERC-20 and VRC-20. Observable metrics include ρ_{audit} , cross-chain configuration hours H_{xchain} , and oracle maintenance frequency. If ρ_{audit} is unchanged, “machine-readable” gains may be offset by cross-chain configuration and oracle maintenance; do not overrate the standard alone.

Section 8 Interoperability with the Ethereum ERC Family

In real deployment, Agents often face Ethereum ERC-20/721 and the Openverse VRC family simultaneously. Only after cross-chain bridges and VTP are delivered as designed can assets flow across ecosystems—until then, configure case by case against production bridges and deployed contracts. Developers should abstract an “asset adapter” at the orchestration layer, unifying homogeneous interfaces across chains into internal types, avoiding hard-binding business logic to chain IDs. Wallets must clearly show “which chain, which standard, what collateral or permission rules the current operation uses,” lest users or Agents mis-send Privcurrency to a public-chain address with no permissioned resolution in a cross-chain transfer.

ERC-20 and VRC-20 can share the same client-library pattern at the Agent code layer; differences are RPC endpoints, contract addresses, and gas tokens. Managing testnet vs mainnet and public vs private configuration is routine enterprise Agent ops—akin to the challenge of wiring enterprise ERP to on-chain contracts.

In cross-chain scenes, the Agent orchestrator must also handle “same name, different chain”: the same brand Privcurrency may deploy one contract on each of two Layer 1 application chains, with different addresses and whitelists (Layer 0 / Layer 1 layering as designed). VTP messages and UNS resolution, if delivered as designed, should return full chain identifiers, lest an Agent spend chain A's balance on chain B's payment. Centralized exchanges' “choose deposit network” has already taught users this lesson; if silicon subjects lack equivalent checks, losses will amplify automatically.

Section 9 Anti-Patterns and Prudent Practice

Several common misuses deserve caution: minting unique NFTs for API calls that should be fungible micropayments—Gas and liquidity costs explode; using unhedged Bitgold or speculative coins as internal enterprise units of account—importing price volatility into operating cost; approving unlimited allowances to malicious contracts—one phishing wipeout; wrongly mapping permissioned-domain Privcurrency into public-chain liquidity pools—breaking whitelist assumptions. Prudent practice includes default minimum-allowance approve, periodic revocation of unused authorizations, permission NFTs default soulbound (non-transferable), isolating stable-settlement assets and utility tokens in separate wallets, and simulating on-chain operations before multisig confirms large transfers.

Section 10 Composition Patterns and Sketch Cases

Three simplified Agent composition patterns for architecture reference—not investment advice, nor audit reports of production systems.

Pattern A: Public-domain data-procurement Agent. The orchestrator holds a contract wallet controlled by a session key and pays a public data DApp per call in a public stable settlement asset (VRC-10 Bitcurrency as Openverse reference instance; counterparts USDC/DAI); each call returns an on-chain receipt event; the session key is destroyed when the task ends. Public stable settlement is chosen because the counterparty is public and must be roughly fiat-comparable; VRC-721 is not chosen because the data interface is fungible and needs no unique slot.

Pattern B: Alliance manufacturing-collaboration Agent. Multiple suppliers on a permissioned chain use the same enterprise-issued Privcurrency; after a robot finishes a process step, the dispatch contract automatically splits to supplier addresses. VRC-11 is chosen because the whitelist is known and flows need not all be public on a public explorer; VRC-721 marks exclusive line-time slots; VRC-13 marks quarterly maintenance service commitments.

Pattern C: Internal R&D quota Agent. Employee-deployed coding assistants consume company-issued VRC-20 DEV_CREDIT, deducting a fixed quota per thousand inference tokens; HR airdrops quotas monthly; non-transferable. VRC-20 rather than stables is chosen because the aim is internal cost attribution, not external payment; regulatorily closer to internal management accounting than issuing a payment instrument to the public.

The three patterns share this: asset type serves governance boundaries and audit needs; “more expensive, more advanced” is not a selection principle. Architecture review should first draw counterparty domains and compliance boundaries, then consult the table above—do not default everything to Bitcurrency or Privcurrency—Openverse instance parameters follow public documentation.

Governance tokens (also often VRC-20) have another role in Agent ecosystems: protocol upgrades, fee-parameter changes, whitelist amendments—Agents themselves usually do not vote, but governance votes held by their operators decide which contracts Agents may access. Separating “pay with stables,” “utility with quota coins,” and “govern with vote coins” avoids everyday micropayments touching the governance attack surface—a lesson many DeFi protocols learned with dual-token structures.

Section 11 Compute Markets and an Engineering Mnemonic

VRC-20 carries divisible utility and quotas; VRC-10 and VRC-11 carry public- and private-domain stable settlement; VRC-721 carries permissions and slots; VRC-13 carries time commitments. When orchestrating, Agents choose asset type by counterparty domain, delivery tense, and scarcity, so every tool call maps to a verifiable on-chain value state.

DePIN networks such as Akash, Render, Bittensor, and io.net already organize compute trade with on-chain orders and stake, but most still price in a single volatile token; Agents must hedge extra to keep stable books; Ballandies et al. (2023) DePIN taxonomy aligns with such compute-market structure².

Technical decision-makers should mark public/private boundaries and VTP routing assumptions on architecture diagrams, configure independent wallets or sub-accounts per asset type, forbid production private keys from entering Agent images in CI/CD, set periodic scans and revocation for approve, and have counsel review boundaries between permission NFTs and security-type VRC-12—these acts do not create security by themselves, but they make implicit assumptions explicit and reduce path dependence on “deploy the VRC suite with a USDT mindset.” An engineering mnemonic: stable settlement choose 10/11; divisible utility choose 20;

unique permission choose 721; time commitment choose 13—concrete instances still require whitelist, collateral state, and compliance labels; a mnemonic cannot replace due diligence; Openverse instance parameters follow public documentation.

注释与引用

- 1. Chapter 6, Section 4, “Verifiable Rules: Execution, State, and History”; Menger (1892) on saleability §§1–2; Chapter 20, Section 9, second emergence dimension. ↩
- 2. Render Network Foundation (2023), *Render Network Whitepaper* v4.0 (GPU render-task settlement; source: official whitepaper v4.0, not independently audited); io.net (2023–2025), official docs (Ray orchestration + Solana settlement); Akash Network Whitepaper (2020); Bittensor Whitepaper (2021); Ballandies et al. (2023), DePIN taxonomy. <https://renderfoundation.com/whitepaper> ; <https://io.net/docs/> ; <https://akash.network/docs/akash-whitepaper/> ; <https://bittensor.com/whitepaper> ↩

§ 23 Robots, Compute Markets, and Autonomous Economies

Foxconn-style long payment terms, cold-chain insurance premiums, and per-second GPU billing point to the same question: can fulfillment events and fund flows bind in the same frame? On-chain patterns couple verifiable signals—“pick complete,” “temperature in range,” “compute slot delivered”—to payment instructions, forming an embryonic autonomous economy: humans set rules; automatic programs contract and settle within those rules. Machine-rule utopias are not under discussion.

Section 1 Robot Fulfillment and On-Chain Payment Triggers

In modern logistics warehouses, autonomous mobile robots (AMRs) pick goods by order and exchange state with central dispatch via API. Traditionally, warehousing fees settle on monthly invoices; fulfillment events and fund flows decouple. An on-chain pattern can couple the verifiable event “pick complete” to a payment instruction: the robot or dispatch contract submits completion proof to an on-chain oracle (barcode-scan hash, weight-sensor reading, vision result); after verification the smart contract transfers a stipulated amount of VRC-11 Privcurrency or VRC-10 Bitcurrency to the service provider—Privcurrency / Bitcurrency here are Openverse reference instances; protocol-neutral counterparts are permissioned-chain enterprise stables or USDC/DAI.

Coupling takes two forms. Atomic: payment and service proof complete in the same transaction or contract call—both succeed or both revert—eliminating one-sided risk of “served but unpaid” or “paid but unserved.” Event-driven: service completes first; off-chain systems periodically batch on-chain—suited to Gas-sensitive scenes, but introduces counterparty risk inside the time window—must be offset by escrow or reputation deposits.

Robots themselves usually hold no private keys; signing authority sits with the deploying enterprise’s contract wallet or operator multisig. Legally, robots remain enterprise assets; fulfillment-quality disputes still point to corporate contractual liability. On-chain payment triggers change settlement latency and audit granularity, not property attribution. Supply-chain “auto-debit after goods receipt” refines, in warehouse-robot scenes, to single pick-task level—financial reconciliation can upgrade from “one monthly invoice” to “one on-chain voucher per task”; CFOs must adjust revenue-recognition timing and tax-filing cadence accordingly.

Unmanned delivery vans, drone drops, and other mobile robots extend fulfillment from warehouses to public roads; liability and insurance grow more complex. “Delivery proof” triggering on-chain payment may come from recipient QR scan, smart-locker door sensors, or dwell time inside a geofence—each proof method has a different fraud surface. Operators should retain a dispute window in the contract: humans may appeal within hours after delivery; only then are funds finally released—a compromise between automation efficiency and consumer protection.

A trap to avoid is “garbage in, garbage out”: if completion proofs can be forged or sensors spoofed, automatic on-chain payment merely accelerates wrong fund transfer. IoT identity, multi-party signed acceptance, and off-chain arbitration clauses remain necessary parts of commercial contracts—technology cannot replace verification of the real world.

Section 2 IoT, Oracles, and Conditional Payments

Cold-chain logistics, agricultural irrigation, industrial predictive maintenance—IoT devices continuously emit environmental data. Insurance and supply-chain finance often bind payment to data thresholds: temperature breach triggers claim; soil moisture met releases the next farm-input tranche. Traditional paths rely on manual

checking and bank transfer; on-chain paths feed data into contracts via oracles and auto-execute transfer when conditions hold.

Agents orchestrate here: monitor multiple device streams, aggregate judgment, call contracts, or submit claim bundles to insurer Agents. Device identity can bind to VRC-721 device keys, ensuring only registered probes' data are trusted by the contract. At high data frequency, putting everything on-chain is unrealistic; rollups or zero-knowledge batch proofs can aggregate off-chain and submit a summary once—the engineering trade-off is the balance of security and cost.

M2M standards versus on-chain conditions: ISO 20022 specifies enterprise-bank messages; ISO/IEC TR 30166 specifies industrial IoT reference architecture; GS1 EPCIS 2.0 tracks logistics events—all three constrain via institutional pipes and device certificates; on-chain historical verifiability is weaker than native on-chain events. Clarification: ISO/NP 23485 was a consumer-IoT privacy-design draft (rejected 2018), not an M2M payment standard—parallel frontier work includes the IETF Machine Payments Protocol (HTTP 402 draft) and the x402 whitepaper¹; the VRC-721 device key + oracle price feed envisioned in the Openverse whitepaper tries to couple “conditional trigger” with “replayable payment,” still pending mainnet validation.

IoT conditional payments, HTTP micropayments, and card-network auto-debit share the M2M stack; constraint-carrier differences are as follows:

Stack position	Representative schemes (2024–2026)	Constraint carrier	Where verifiability lands	VRC	Observable metrics
HTTP micropayments	x402 (2025.05; x402 Foundation 2025.09)	Reputation	On-chain receipt replayable; policy with facilitator	VTP + VRC-20 per-call quotas / VRC-10 stable settlement	Pilot success rate, γ_{gas}
Custodial wallet	AgentKit (2024.11 CDP)	Reputation	Multisig/session keys partly on-chain readable	Contract wallet + UNS whitelist + VRC asset policies	Custodial mispay rate r_{mispay}
Card auto-debit	agentic commerce (AP2/A2A, Visa TAP, Mastercard Agent Pay)	Reputation	Authorization logs inside institutions	On-chain sub-ledger + Privcurrency month-end reconciliation	Auto-debit dispute rate, τ_{revoke}
Industrial M2M messages	ISO 20022 camt/pacs, ISO/IEC TR 30166, GS1 EPCIS 2.0	Reputation	Messages mutable off-chain	VTP messages + VRC-721 device keys + oracle event hashes	Event-payment mapping completeness, false-trigger rate
Instant fiat pipes	FedNow / RTP / SEPA Instant (2023–2025)	Reputation	24x7 fiat instant; weak on-chain receipt	VTP + on-chain receipt mapping	End-to-end latency, reconciliation discrepancy rate

The regulatory implication of conditional payment: if insurance claims and loan disbursements trigger purely by code, courts in dispute must interpret whether “the code accurately expressed the parties’ intent.” Some jurisdictions already recognize smart contracts as a mode of contractual performance, but case law remains thin. Before full auto-trigger, enterprises should retain human override windows and multisig pause rights for material disputes—consistent with guardian multisig pause logic.

Section 3 Compute Markets, DePIN, and GPU Slots

Large-model inference and scientific computing consume GPU time; supply and demand swing sharply by time and task type. Centralized clouds price reserved, on-demand, and spot instances; on-chain compute markets try to represent slots as tradable assets: sellers stake or lock VRC-721 slot NFTs, committing compute over a specified block range; buyers pay Bitcurrency or Privcurrency; failure to deliver on time slashes the deposit—Openverse slot + stable-settlement combination is a design proposal pending mainnet validation; the following discussion applies equally at the protocol-neutral layer to DePIN networks already running.

In 2024–2026, DePIN compute markets already supply comparable instances. Ballandies et al. (2023) layer DePIN by physical resources—compute, storage, wireless coverage: Akash/Render/io.net are compute-type, Helium wireless-type, Filecoin storage-type; most networks still price in a single volatile token, so Agents must hedge extra to keep stable books². As with HTTP micropayments and custodial wallets, DePIN shows payments can be replayed on-chain; whether delivery is independently verifiable remains the weak link—compute markets are the testing ground of the verifiability thesis: liquidity and compute depth embody saleability; whether delivery hashes, slash records, and stable-settlement layers can be independently re-checked embodies verifiability.

Network	Settlement and constraint	Constraint carrier	With VRC	Verifiability gap	Observable metrics (2024–2026)
Akash	On-chain order book; AKT stake bids GPU/CPU	Stake slash + order book	VRC-721 slots + VRC-10 stable settlement	Delivery proofs off-chain; volatile-token pricing	Order fill rate, SLA breach rate
Render	RNDR settles per render task; output-hash acceptance	Token incentives + hash acceptance	VRC-11 private compute pools + VRC-20 internal quotas	Acceptance depends on render output; pricing volatile	Share of task-acceptance disputes
Bittensor	Subnet TAO stake and inference scoring	On-chain registration + slash	VRC-20 subnet quotas + soulbound reputation	Sybil and score-manipulation risk	Subnet slash frequency, manipulation detection rate
ERC-8004 Agents	Ethereum-ecosystem draft (2025); on-chain Agent registry + reputation interface	On-chain registry + reputation fields	VRC-20 subnet quotas + soulbound reputation	Off-chain delivery hard to re-check independently	Sybil share, reputation–delivery gap
io.net	IO token incentives; aggregates idle GPUs	Stake + off-chain delivery proofs	VRC-721 slots + stable-settlement layer	Node uptime and compute delivery separable	Uptime vs actual delivery gap Δ_{deliver}
Helium	HNT/IOT/MOBILE incentivize IoT/5G hotspots	PoC coverage proofs + oracle feeds	VRC-721 device slots + stable settlement	Off-chain wireless coverage hard to re-check independently	Hotspot uptime vs actual coverage gap
Filecoin	FIL incentivizes decentralized storage; Proof-of-Replication	Space–time proofs + stake slash	VRC-721 storage slots + VRC-10 settlement	Storage delivery verification weaker than payment	Storage fault rate, retrieval latency

The table focuses on DePIN compute and storage layers. Compute-side constraint is mainly stake slash; HTTP micropayments and card auto-debit remain reputation-layer; the parameter layer (4337 policies, PCIM collateral queries) is the gap VRC tries to fill. As buyer, an Agent can auto-bid spot compute by task-queue length; as seller, it can list idle GPU slots, with contracts settling per second or per epoch. On-chain reputation scores (historical delivery rate, latency distribution, complaint events) affect ranking and deposit requirements—

reputation data themselves come from verifiable on-chain history, harder to unilaterally tamper than internal platform scores, yet still pollutable by Sybil attacks, so stake and identity permissioning must combine. DePIN networks show that silicon compute trade can occur without traditional cloud accounts; bottlenecks are that volatile tokens struggle as units of account, and delivery-proof verifiability is weaker than payment itself—the division stable settlement (VRC-10/11) + slots (VRC-721) is precisely the engineering proposal aimed at that gap³.

Monetary choice in compute markets: public open markets lean to VRC-10 or protocol-neutral USDC/DAI for cross-provider comparison; internal enterprise compute pools may use VRC-11 or internal VRC-20 quota coins to avoid internal scheduling shocking public prices. Linking to fiat cloud bills still needs month-end aggregation—tax and capitalization policy have no mature template yet for “per-second on-chain micropayments.”

Auctions and order books are two engineering implementations of compute pricing. Order books suit long listings and transparent price discovery for GPU SKUs; Dutch auctions or per-second bidding suit spot slots; Agents can auto-bid by queue depth. Honesty of on-chain auctions depends on stake and delivery proofs: undelivering sellers lose deposits; malicious bidding buyers bear Gas and opportunity cost. Versus traditional cloud spot instances, on-chain markets’ advantage is public rules and cross-vendor comparability; disadvantages are thinner liquidity and higher ops complexity—for the foreseeable years, the two will coexist rather than substitute.

If DePIN + stable-settlement layering beats “single volatile-token pricing,” then under the same GPU SKU and similar utilization, Agent schedulers that book internally in VRC-10/11 (or USDC) should show lower ops-cost volatility σ_{ops} (standard deviation of monthly compute bills in fiat) than schedulers that settle directly in AKT/RNDR/TAO/IO—testable in 6–12 month hybrid cloud–DePIN pilots. Observable metrics include σ_{ops} , uptime vs actual delivery gap Δ_{deliver} , and SLA breach rate. If σ_{ops} shows no significant difference, the marginal value of the stable-settlement layer should be narrowed to accounting convenience, and risk-reduction claims withdrawn.

Testable proposition (delivery verifiability): If compute markets’ verifiability bottleneck is off-chain delivery rather than payment, then among Akash/Render/Bittensor and similar networks, suppliers whose delivery proofs are independently re-checkable (output hashes, space–time proofs queryable on-chain) should show shorter post-SLA-breach dispute mediation time τ_{dispute} than suppliers relying only on internal platform scores—comparable on a 12-month order-book panel. Observable metrics include τ_{dispute} , Δ_{deliver} (uptime vs actual compute delivery gap), and slash-event frequency. If τ_{dispute} shows no significant difference, the claim that “stake slash completes delivery verifiability” should be narrowed to a payment-layer advantage.

Section 4 Multi-Agent Collaboration and On-Chain Reputation

Complex tasks often require division among Agents: retrieval, analysis, drafting, compliance review. Centralized orchestration platforms can book each Agent’s contribution internally; decentralized orchestration needs verifiable splits and portable reputation accumulation. Automatic contract splits solve current revenue division; reputation portability is the longer open-collaboration problem.

On-chain reputation can be designed as non-transferable soulbound tokens or registry fields recording completion counts, default counts, and mean response time. Downstream Agents, when choosing upstream skills, query reputation thresholds and refuse collaboration below them. This resembles e-commerce seller ratings, but data come from on-chain events rather than platform databases—cross-platform portable reputation is a potential dividend of an open Agent economy, and also a governance hard problem of privacy and retaliatory bad reviews.

Reputational constraint hangs on internal platform scores; third parties cannot re-check independently. Verifiable constraint requires that reputation scores trace to replayable on-chain events (delivery hashes, slash records, split receipts), not black-box stars. If a soulbound field is written by only one contract, Sybil pollution remains possible; stake and identity permissioning must combine. Bittensor subnet slash and Akash stake forfeiture are embryonic verifiable constraints; pure off-chain delivery proofs still hang on reputation—DePIN and VRC layered design (721 slots + 10/11 stable settlement) try to fill that gap.

Multi-Agent collaboration must also solve the liability chain: if a drafting Agent cites a false source from a retrieval Agent, who bears the harm? On-chain logs can prove “the retrieval Agent returned hash H at block N,” but cannot automatically prove that H’s content is true. Ultimate carbon-based responsibility cannot be erased; on-chain records’ value is lowering the cost of proof—human guardianship cannot abdicate.

Section 5 Boundaries of the Autonomous Economy

“Autonomous economy” is easily misread as machines independently owning property and legal personality. A pragmatic definition: within rules, quotas, and tool whitelists preset by carbon-based subjects, silicon systems may autonomously discover counterparties, contract, pay, split, and renew—without stepwise human clicks. Autonomy is a spectrum: from scheduled batch scripts, to Agents adjusting procurement by market signals, to multi-Agent games in labs—the right end is riskier and must be adopted more cautiously.

Robot picking, sensor-triggered claims, and compute bidding all must answer “who pays under what rules.” In Menger’s era, saleability decided whether a thing could become a medium of exchange; in the silicon era, the verifiability threshold—operationalization of Chapter 6, Section 4’s three layers of “execution–state–history” in Agent scenes—decides whether a program can accept a counterparty’s asset at millisecond scale. Readable collateral ratios, on-chain queryable whitelists, and replayable delivery hashes are the key to partly replacing reputational constraint (“trust this cloud vendor”) with verifiable rules. $\text{Monetary emergence} \approx \text{saleability ranking} \times \text{verifiability threshold}$; whether non-human subjects can enter value transfer under public rules is a question silicon monetary theory must face—Openverse/VRC serve only as engineering contrast. The boundary lies in whether carbon-based guardians can read the rules before an incident and assign responsibility after; spending policies and asset whitelists are the concrete operating face of that boundary.

Hayek, discussing competitive money, stressed dispersed information and local knowledge; the autonomous economy extends that logic to the execution layer—field sensors know better than HQ ERP whether a cold store lost power; local Agents know better than HQ finance when emergency spare parts must be bought. If money and value interfaces cannot reach the silicon layer, local knowledge cannot convert into timely payment—“autonomy” remains information processing without economic consequence.

The boundary: operations involving life and health, critical infrastructure, or systemic financial risk should not be fully autonomous. National graded regulation of algorithmic trading, autonomous driving, and medical AI offers analogous frames—the autonomous economy must accept industry licensing, log retention, and human-takeover duties.

Section 6 Liability and Regulation: Who Answers for Autonomous Systems

When an autonomous Agent or robot causes property damage—wrong transfer, wrong shipment, wrong contract signature—victims first ask: who pays? Current law tends to trace to natural persons, legal persons, and their employees or agents; the silicon subject itself is not the defendant. Whether a deployer who proves reasonable security configuration may mitigate liability has no unified standard across countries. Whether

product-liability “defective product” covers “a buggy smart contract” or “a prompt-injected model” is still early in case accumulation.

Regulatory tools include: mandatory KYC and beneficial-owner registration (linking off-chain identity to on-chain addresses), large and suspicious-pattern reporting, address freezes on permissioned chains, and licensing requirements for “public-facing fund-custody Agents.” Structural tension exists between censorship-resistant public-chain autonomous payment and regulatory demands; a fully permissionless autonomous economy is hard to scale legally in mainstream jurisdictions. The compliance path is a combination of permissioned domains, quota limits, and auditable logs—not hoping one tech stack simultaneously satisfies “fully permissionless” and “fully compliant.”

Insurance markets may spawn “Agent operations cover” and “smart-contract error cover,” dispersing tail risk through markets—provided losses are measurable and historical data can accumulate. As with traditional cyber insurance, moral hazard (deliberately deploying high-risk Agents to arbitrage insurance) must be restrained by deductibles and audit clauses.

Emerging legislation such as the EU AI Act imposes logging, human oversight, and transparency duties on high-risk automated systems—on-chain auditable logs may be a compliance asset rather than a burden, provided personal data are minimized and GDPR-class privacy rules are met. China’s current rules on generative-AI service filing and algorithmic recommendation may also extend to Agents that “can pay on users’ behalf”: who provides the entry point and who bears real-name authentication will decide whether on-chain wallets can face the domestic public. Specific articles change with legislative revision; autonomous-payment features raise the regulatory attention grade and must enter compliance assessment at product-design time, not as post-launch remediation.

Section 7 Employment, Division of Labor, and Retraining

Social debate on the autonomous economy often points to job displacement. Warehouse robots, automated customer service, and code-generating Agents do compress some role demand while creating new trades in robot ops, prompt engineering, on-chain compliance, and oracle operations. Economic history shows technological shocks are first structural reallocation, not instantaneous mass unemployment; policy focus is retraining speed and social safety nets, not banning automation itself.

Monetary popularization and employment have no direct causal link: protocols lower the threshold of value transfer, not wage levels. But if on-chain micropayments make fragmented labor easier to price and compose, gig and micro-task markets may expand—combining personal time tokens (VRC-13, reference instance) with public stable settlement (VRC-10, reference instance) lowers friction in “selling professional hours,” a possible marginal improvement for freelancers. Optimistic and pessimistic forecasts both need longer time-series evidence; no verdict is entered here.

Section 8 Energy, Environment, and Sustainability Questions

Compute-market expansion brings energy controversy. On-chain settlement itself consumes energy, but usually far less than training large models or running data-center main loads; environmental criticism targets proof-of-work consensus or inefficient redundant computation more. Openverse documentation designs for PoS and Layer 0 / Layer 1 layering—Layer 0 bears consensus and cross-domain settlement anchoring; Layer 1 carries application load—if delivered as designed, it may lower energy footprint per transaction—concrete parameters must update with mainnet measurement; static claims of “green” are unwarranted.

If the autonomous economy drives disorderly compute-bidding expansion, it may raise regional electricity prices and carbon emissions. Carbon-account tokens, on-chain renewable certificates (RWA-class VRC-12 applications), and similar attempts try to partly internalize externalities; effectiveness depends on whether regulators recognize on-chain carbon credentials. Agent orchestration layers may include policies to “prefer low-carbon hours or green compute pools,” expressing corporate ESG preference—provided disclosure standards are credible.

Section 9 Pilot Paths: From Sandbox to Production

If enterprises consider moving robot or Agent on-chain settlement from experiment to production, a pragmatic path is staged opening: first on testnet or consortium-chain sandboxes with test tokens of no real fiat value, validating contract logic and ERP integration; then small-value Privcurrency pilots on private mainnet, limited to a single warehouse or single API product line, with daily spend caps and human weekly reports; only after fiat on/off-ramp channels with compliant custodians and exchanges are established should on-chain flows enter formal accounting and tax filing. Skipping the first two stages for large public-chain experiments is unwise on both regulatory and operational risk.

Sandbox stages should define success criteria—mispay rate, reconciliation discrepancy, mean settlement latency, Gas or fees as a share of revenue, and security-incident count—and not expand until criteria are met. On-chain settlement’s weak reversibility means one configuration error’s fund loss may exceed years of fee savings.

Multinationals must also handle multi-jurisdiction Agent deployment: the same orchestration logic may need extra AI decision logs in the EU, and in some regions must confine on-chain payment to permissioned private chains. Ambition for “one global contract set” often collides with “one compliance pack per locale”; architecture should use modular compliance plugins rather than hard-coding a single legal assumption. Whether enterprises will bring internal API markets and automated spend onto permissioned chains often depends on organizational friction more than technical feasibility—Treasury and private-domain settlement capacity must sink to sub-Agents and sub-devices before robot and compute scenes can deliver.

Section 10 Port Unmanned Fleets and Multi-Currency Positions (Case Sketch)

The following uses Openverse VRC asset names as reference instances, not audits of production systems; the same logic maps to running standards such as USDC/ERC-20.

Imagine a port operator deploys a “dispatch Agent”: after unmanned tractors finish container short-haul, sub-accounts pay yard charging stations in Privcurrency (permissioned whitelist); pay tiny Bitcurrency to third-party weather APIs (public services); hold VRC-721 meaning “passed today’s safety patrol” before accepting jobs; consume VRC-20 dispatch quota coins to stop any single instance from issuing unbounded tasks. Parent-company Treasury tops up hot wallets daily from fiat; month-end matches on-chain flows to cost centers—multiple VRC tools stack here rather than relying on a single asset type.

The sketch also shows **failure recovery**: when public Bitcurrency liquidity is thin, the dispatch Agent may switch to local data sources under signed long-term Privcurrency contracts, or pause external calls and alert human on-duty staff. Autonomy does not mean uninterruptible; carbon-based guardians’ pause switches and on-chain circuit breakers should be default configuration.

Section 11 Data-Factor Markets and Hidden Bills

Data itself can be commoditized: on-chain markets list dataset access rights; buyer Agents purchase with Bitcurrency or stream-pay per query (Openverse public stable settlement as reference instance; protocol-neutral counterparts USDC/DAI); sellers represent exclusive licenses with NFTs. Data-quality disputes still depend on off-chain audit; what the chain hardens is payment and data-hash commitments—enough for accounting provenance, not a guarantee that content is true.

Robot and compute clusters also consume power and bandwidth. Smart-meter readings on-chain can trigger Privcurrency splits; finance can ask “how much power and compute did order #8842 consume,” rather than only monthly total electricity. When IoT oracles are tampered with, the chain will faithfully execute wrong inputs—guardians must retain off-chain spot-check rights. Energy and data as two classes of “hidden bills” are cost lines an autonomous economy cannot omit when moving from demo to scale.

Section 12 Stake, Insurance, and Second-Layer Markets

Pure on-chain settlement cannot eliminate counterparty risk: sellers take payment without delivery; compute sellers misreport specs. Traditional e-commerce relies on platform guarantees and credit-card chargebacks; on-chain relies on stake, delayed release, and insurance pools. Before Agents join compute markets, they may require sellers to lock stable-settlement collateral (VRC-10 Bitcurrency as Openverse reference instance; counterparts USDC/DAI)—VRC-12 (Bitsecurity) is a security token, not Agents’ default settlement or performance-stake path; when evaluating VRC-10 instances, procurement Agents should read C_0 and Bright-PCIM peg-bound variables on-chain rather than apply Maker-style liquidation-line logic. Dispute windows are handled by arbitration contracts or off-chain terms. Reputation systems put historical performance on-chain; procurement Agents auto-weight quotes—permissioned Privcurrency networks build credible reputation more easily via KYC; public open markets must resist Sybil attacks.

On the insurance side, parameter errors causing large Agent mispayments get a premium framework—maturity is limited; enterprises more often self-insure with low-balance hot wallets and multisig cold reserves. Stake, reputation, and insurance form a second-layer market that, together with on-chain wallets, asset standards, and automatic splits, supports the machine economy; missing any layer, the system falls back to centralized prepay or human approval.

注释与引用

1. GS1 (2024), EPCIS 2.0 standard; ISO/IEC TR 30166:2020 (industrial IoT reference architecture); ISO/NP 23485 (rejected 2018, consumer-IoT privacy draft, not M2M payment); IETF, draft-ryan-httpauth-payment-00 (Machine Payments Protocol, HTTP 402 semantics); Coinbase (2025), x402 Whitepaper (source: official whitepaper, not independently audited); Coinbase Developer Platform (2024.11), AgentKit docs; Google (2025), Agent Payments Protocol (AP2); Visa (2025), Trusted Agent Protocol (TAP); Federal Reserve (2023–2025), FedNow Service docs. <https://www.gs1.org/standards/epcis> ; <https://www.iso.org/standard/53211.html> ; <https://datatracker.ietf.org/doc/draft-ryan-httpauth-payment/> ; <https://www.x402.org/x402-whitepaper.pdf> ; <https://docs.cdp.coinbase.com/agentkit/docs/welcome> ; <https://github.com/google-agentic-commerce/AP2> ; <https://developer.visa.com/capabilities/trusted-agent-protocol> ; <https://www.frb.services.org/financial-services/fednow> ↩
2. Ballandies, Mark, et al. "A Taxonomy for Blockchain-based Decentralized Physical Infrastructure Networks (DePIN)." *Frontiers in Blockchain* 6, 2023, 1272380 (compute/storage/wireless DePIN taxonomy); Mohan, Deepak. "Decentralized Physical Infrastructure Networks (DePIN)." Messari Research, June 2023; Easley, O'Hara & Basu (2024), "From mining to markets: The evolution of bitcoin transaction fees," *Journal of Financial Economics* 169, 103892 (P2P ledger → market

pricing evolution; contrast with DePIN compute auction pricing). <https://doi.org/10.3389/fbloc.2023.1272380> ; <https://messari.io/report/decentralized-physical-infrastructure-networks-depin> ; <https://doi.org/10.1016/j.jfineco.2024.103892> ↩

3. Akash Network Whitepaper (2020; source: official whitepaper, not independently audited); Render Network Foundation, *Render Network Whitepaper* v4.0 (2017/2023; source: official whitepaper v4.0, not independently audited); io.net Docs (2023–2025; source: official docs, not independently audited); Helium Foundation Docs (2023, IoT/5G DePIN; source: official docs, not independently audited); Protocol Labs, *Filecoin: A Decentralized Storage Network* (2017/2022; source: official whitepaper, not independently audited); Bittensor Whitepaper (2021; source: official whitepaper, not independently audited); Ballandies et al. (2023), "A Taxonomy for Blockchain-based DePIN," *Frontiers in Blockchain* 6, 1272380; Mohan (2023), Messari "Decentralized Physical Infrastructure Networks (DePIN)." <https://akash.network/docs/akash-whitepaper/> ; <https://renderfoundation.com/whitepaper> ; <https://io.net/docs/> ; <https://docs.helium.com/> ; <https://filecoin.io/filecoin.pdf> ; <https://bittensor.com/whitepaper> ; <https://doi.org/10.3389/fbloc.2023.1272380> ↩

Part VII: The Popularization of Money

§ 24 Protocol Collaboration and State Monopoly

30-second chapter: State monetary monopoly is rooted in the tax anchor, lender of last resort, legal tender, and network effects; protocol collaboration lowers participation costs through verifiable rules and interoperability—the two will long coexist, not as either-or. PCIM puts issuance discipline on-chain readable; circulation-tier referenda decide when to relax the mint output rate—rejection leaves the tier unchanged. Openverse is one deployment sample of PCIM.

The structural tension between protocol collaboration and state monetary monopoly should neither be optimistically judged as inevitable victory nor pessimistically dismissed as impossible—it must be examined within a single coordinate system.

Section 1 The End of the Island Era and the Rise of Interoperability Infrastructure

The European Union’s Markets in Crypto-Assets Regulation (MiCA, effective 2024) requires stablecoin issuers to hold reserves and disclose audits, drawing a compromise zone between sovereign regulation and permissionless protocols—here the friction between state monopoly and protocol collaboration becomes concrete.

Early blockchain ecosystems were extremely fragmented. Bitcoin, Ethereum, and various public chains each guarded their own territory, with almost no native channels for value transfer between them. A token on Ethereum wishing to enter the Bitcoin network had to pass through a centralized exchange as a single point of mediation; every cross-chain step meant a transfer of trust and accumulation of counterparty risk. This situation is structurally strikingly similar to medieval Europe, where mints proliferated and city-state currencies did not circulate across borders—technologically novel, yet economically friction remained high.

Efforts to change this pattern concentrated on building interoperability infrastructure. Cosmos’ s IBC (Inter-Blockchain Communication protocol), Polkadot’ s parachain mechanism, cross-chain hubs in the Ethereum ecosystem, and Openverse’ s designed Layer 0 value-exchange layer with VTP (Value Transfer Protocol) and the VRC suite attempt, from different technical paths, to solve the same problem: let value be addressed and delivered like email, without caring which chain or virtual machine runs underneath.

VTP (Value Transfer Protocol) abstracts value transfer as a network-layer protocol, defining unified address formats, message structures, and routing rules so that assets on different chains can recognize and exchange one another through standardized messages—the whitepaper analogizes it to email routing: value can be addressed and delivered across domains like `name@domain`. The VRC suite specifies interface standards for token classes at the application layer, from public-domain money (VRC-10) to private-domain stablecoins (VRC-11), asset securities (VRC-12), and time tokens (VRC-13), sharing one composable interface language. Openverse is positioned as Layer 0—a global decentralized value-exchange layer: at the protocol layer it coordinates POS consensus, validator staking (Bitgold), cross-domain clearing anchors, and VTP routing; Ethereum, Cosmos chains, consortium chains, and ecosystem application chains connect as Layer 1 to this exchange layer rather than being locked into subnets under a single Hub. In whitepaper engineering terms, the Hub Chain corresponds to the Layer 0 core chain and Zones to native Layer 1 application chains within the ecosystem—the two implement layering, not the full boundary of the architecture. VTP and UNS (Universal Name Service) jointly reduce addressing friction across chains and ecosystems, so protocol collaboration need not build bespoke bridge logic for every chain pair.

The strategic significance of interoperability infrastructure is that it fundamentally changes the cost structure of multi-currency participation. In the island era, issuing a new token meant simultaneously building

independent wallets, liquidity pools, and settlement channels; in the interoperability era, new units can plug into existing routing and liquidity networks, with marginal cost falling sharply. Historically, every decline in bookkeeping and clearing costs opened a window for new participants to enter monetary affairs—from commercial paper to electronic payments, none differed. The impact of protocol standardization on monetary participation thresholds follows the same historical logic, only compressing the time scale relative to the gradual diffusion of commercial paper and electronic payments.

Liquidity accumulation is the key variable for interoperability infrastructure to deliver value. However perfect the routing protocol, without sufficient liquidity depth, actual slippage on cross-chain trades will offset theoretical fee savings. Liquidity accumulation depends on market makers' active participation and user-base growth, with a chicken-and-egg bootstrap problem between them. Incentive design—liquidity mining, protocol fee sharing, governance-weighted liquidity—is the engineering means to solve this bootstrap problem. But incentive distortion (such as capital withdrawal after liquidity mining ends) is also a common real cost. Truly sustainable liquidity must ultimately come from genuine transaction demand, not short-term incentive-driven profit-seeking. Maturity of interoperability infrastructure is therefore not merely perfection of protocol specifications but the process by which real economic activity accumulates on-chain.

Yet interoperability infrastructure is not a free lunch. Cross-chain bridges have become the most concentrated attack surface in recent years, with billions of dollars lost to bridge vulnerabilities. Routing complexity introduces new layers of trust: using the VTP protocol requires trusting that the node network executing routing will not collude at a given moment. Technological empowerment and technological risk are two sides of the same coin—a point that must stay clear when discussing challenges to state monopoly. Interoperability's maturity must withstand sustained attack by real adversaries, not remain at “design complete” in technical papers. The historical record of bridge security requires designers and users, when optimistically citing the interoperability vision, to retain prudent questioning of engineering implementation quality.

Section 2 The Institutional Foundations of State Monetary Monopoly

To judge how far protocol collaboration can shake state monetary monopoly, one must first see how deep the latter's roots run. State monetary monopoly is not maintained by coercion alone—it is embedded in modern society's infrastructure and, to a considerable degree, has economic rationality.

Taxation forms the deepest demand anchor. Georg Friedrich Knapp, in *The State Theory of Money*, first defined money as the state-established “unit of account”: so long as sovereignty defines taxes and public payment obligations in domestic currency, economic subjects must hold that symbol in cash flows—monetary value comes from state bookkeeping rules, not from commodities' intrinsic properties¹. A. Mitchell Innes approached from another angle: money's essence is transferable credit–debt clearing relations; “money is not a thing but a law”—state tax obligations create an acceptance circuit, not intrinsic value in the commodity itself². Knapp and Innes are often grouped as chartalists, but the dialogic tension is that the former stresses the sovereign unit of account and the latter credit clearing; Goodhart summarizes this as the long coexistence of M-money (unit of account/legal tender) and C-money (medium of circulation/store of value)³. Randall Wray, in the MMT framework, pushes this logic to the policy level: one main function of taxation is to create rigid demand for domestic currency, enabling a fiscal cycle of “spend first, recycle later”⁴; Bell (Kelton) further explains at the operational level that taxation recycles reserves and adjusts the interest-rate corridor in day-to-day central-bank–Treasury operations, rather than “financing” spending in an accounting sense—contrasting with the folk intuition that “government must have money before it can spend,” yet not removing inflation as a real constraint⁵. On the

surface these are administrative clauses; in substance they embed fiat into every taxpayer's and wage-earner's daily cash flow; once the anchor is firm, network effects self-reinforce.

In crisis moments, lender-of-last-resort functions provide another endorsement of fiat monopoly. Bagehot, in *Lombard Street*, proposed that in liquidity panics the central bank must “lend freely at a penalty rate on good banking securities”—distinguishing liquidity crises from solvency crises, trading systemic stability for limited rescue of individual institutions⁶. Goodhart, in the natural history of central banks, traces that lender-of-last-resort functions were not written into law from the start but were *ex post* institutional inventions recognized through repeated runs and panics—their rationality comes with moral hazard and must be understood jointly with deposit insurance and prudential supervision⁷. Mehrling summarizes the post-2008 Fed as “dealer of last resort”: in crisis it must supply repo and market-making liquidity to the entire shadow-banking system—Bagehot's “lend on good collateral” has expanded to injecting tradability into the market itself⁸. The Fed's balance-sheet expansion in 2008 and 2020 stretched this function far beyond the traditional banking system; experience from successive shocks shows that even when long-term costs are substantial, short-term buffering is still regarded as a legitimate reason for central banks to exist. Protocol tokens have no institutional counterpart bearing this duty—on “Black Thursday” in March 2020, MakerDAO's liquidation spiral and the Fed's same-day liquidity injection formed a contrast: Maker and similar CDP schemes can automatically force liquidation at line *L*; VRC-10/PCIM sets no *L/W*; under extreme market stress the pressure path is redemption runs plus reserve depletion; on-chain protocols can pause minting or circuit-break, but no one bears the obligation of unlimited injection on state credit⁹. This is a structural weakness of protocol money in robustness reputation, which this book does not evade.

Legal apparatus writes fiat into modern society's measuring system: contract pricing, debt discharge, litigation damages—all nodes use fiat as the yardstick. Replacing fiat is not merely a technical migration but a systematic rewrite of legal texts; financial statements, insurance actuarial work, and pension plans are all built in fiat units. Habit and legal language change on decadal scales, not quarterly ones.

Habit and cognitive anchoring are equally hard to shake. Wage bargaining, housing prices, long-term saving—within a few generations, internalized purchasing-power expectations build fiat's “defaultness.” Monetary network effects exceed ordinary commodity markets—the more users, the higher each subject's switching cost. Cognitive anchoring will not loosen from a technology demo; it can only be slowly rewritten through accumulated experience and generational turnover.

Seeing these four layers of foundation, the aim is not to prove monopoly impregnable but to calibrate expectations: protocol collaboration's impact on state monetary monopoly will be long-term, gradual, and marginal—not short-term institutional replacement. Every protocol design that tries to bypass these foundations either meets resistance in reality or lacks sufficient adoption momentum at the social level.

State monetary monopoly must also confront four strongest academic defenses—chartalism, lender of last resort, New Keynesian inflation targeting, and MMT fiscal space.

Chartalism: does the tax anchor imply monopoly mint prerogative? The strongest Knapp–Innes–Wray tradition holds that without sovereign unit of account and tax recycling, private or protocol money is only tradable IOUs, permanently marginal in retail and public finance. This book accepts half and questions the other half: the tax anchor indeed explains domestic daily pricing and public-spending dominance—the book's thesis presumes long coexistence of state money and does not dispute this fact. Goodhart (1998) notes that chartalism and metallism describe different dimensions of money—the former explains unit of account and legal tender, the latter store of value and cross-border settlement—the two long coexist; debate should shift from “what is money” to “who

guarantees clearing recycling and whether rules are third-party verifiable”³. But “rigid domestic-currency demand” explains fiat usage volume, not automatically monopoly mint prerogative at a single central bank. Historically commercial paper, the Eurodollar market, and contemporary cross-border stablecoins all expanded beyond legal tender and tax anchors; voluntarily adopted verifiable collateral units need not wait for legal-tender status. Brunnermeier and Niepelt further show in models that under appropriately designed fiscal–central-bank division, private and public money can be equivalent in equilibrium—the key is not whether the state issues but whether the same clearing and recycling mechanisms are satisfied¹⁰. Equivalence is not unconditional: it requires (i) private units freely convertible to the public anchor; (ii) fiscal recycling of liquidity overflow under credible rules; (iii) shared unit of account or stable peg—missing any condition, parallel currencies degenerate into non-interconvertible IOU markets, not true money within a Knapp-style acceptance circuit. This aligns with this book’s layered claim: protocol units perform C-money (medium/store) functions in high-friction scenes without denying the tax anchor of domestic M-money (unit of account/legal tender). This tensions with Knapp-style “only state money is real money”: if equivalence holds within bounds, debate should shift from ontology (what is money) to institutional theory (who guarantees liquidity recycling and whether rules are third-party verifiable)—the book unfolds its argument on the latter plane. The protocol path offers optional pricing layers and auditable issuance discipline, not overnight replacement of tax obligations.

Lender of last resort: can protocols substitute crisis liquidity? No—as above, this is a boundary both this book and Mr. Hayek’s competitive-money theory must face. If a March 2020-style synchronized deleveraging recurs, on-chain protocols have only circuit breakers, reserve depletion, and governance pause—no Bagehot-style subject of “unlimited injection on state credit”—the same-day Maker liquidation spiral versus Fed balance-sheet expansion shows: protocols can automatically execute rules, not automatically create sovereign liquidity. Calomiris, from banking-crisis history, notes that lender of last resort and deposit insurance ease panic while accumulating moral hazard and political capture—monopoly mint prerogative’s “rationality” carries “costs” and cannot one-sidedly veto the protocol path¹¹. When fiat liquidity and on-chain redemption depth may both dry up in crisis, whether PCIM redemption queues maintain orderly exit still requires stress data. The above does not claim “protocols replace central-bank crisis functions,” only that in specific scenes verifiable overcollateralization and on-chain auditable mint/redeem rules (VRC-10 rules see glossary) substitute part of “implicit seigniorage plus opaque balance-sheet expansion”; macro lender of last resort remains complementary division between state layer and protocol layer, not either-or.

New Keynesianism: does the welfare foundation of the 2% inflation target foreclose protocol competition? Woodford, in *Interest and Prices*, argues that with downward nominal wage and partial price rigidity, moderate positive inflation (about 2%) buffers relative-price adjustment and lowers the probability of hitting the zero lower bound¹². Rotemberg and Woodford (1997) embed the same logic in an estimable DSGE framework, turning FIT from normative claim into backtestable policy-evaluation language¹³—strengthening “2% has welfare foundation” yet not deriving that non-central-bank issuers may not participate: welfare argument targets macro stabilizer configuration, not seigniorage exclusivity itself. Galí formulates flexible inflation targeting (FIT) as incorporating the employment gap in the reaction function, claiming the discretionary framework already internalizes distributional concerns¹⁴; Clarida–Galí–Gertler call this framework New Keynesian “science,” formalizing central-bank reaction functions as systematic responses to inflation and output gaps¹⁵. Bernanke et al.’s empirical summary of multi-country inflation targeting binds the 2% anchor with expectation management and transparent communication as institutional consensus¹⁶; Eggertsson and Woodford further show that under the zero lower bound, optimal policy must tolerate higher average inflation or unconventional tools—explaining why FIT became global central-bank standard after 2008¹⁷. Blanchard, Dell’Ariccia, and Mauro, in post-crisis reflection, ask

whether if the ELB becomes normal rather than exceptional, 2% remains optimal average inflation—a higher target leaves more room to cut policy rates but costs steady-state welfare loss and harder expectation management¹⁸; Schmitt-Grohé and Uribe show that under ELB constraints, optimal policy often must tolerate temporary inflation overshoot or rely on fiscal coordination—this does not foreclose protocol competition but shows macro stabilizers are a multi-tool joint problem that fixed collateral parameters cannot replicate¹⁹. This book does not dispute the Woodford–Galí consensus here; what it disputes is only that optimal macro stabilizers derive permanent closure of mint participation. If this defense holds, fixed rules or on-chain collateral parameters are indeed welfare-inferior on macro-stabilizer functions—this book accepts FIT as among best practices within sovereign fiat systems; what it questions is whether monopoly mint prerogative is therefore unchallengeable. The 2021–2022 “transitory inflation” misjudgment shows discretionary frameworks likewise depend on model form and political windows; Sargent, in *The Conquest of American Inflation*, also records that even after Volcker-style tightening succeeded, expectation anchoring still requires sustained institutional and political maintenance²⁰. Cantillon effects leave distributional consequences long underestimated. The protocol-side contribution is moving issuance constraints from conference rooms to on-chain state machines: current-tier collateral ratio C_0 , mint output rate σ , circulation-tier referendum progress, and mint/redeem rules are readable by any third party; tier upgrades require vote approval—failure leaves the original collateral ratio unchanged; crisis tightening can separately go through referendum to raise C_0 (Chapter 14, Section 2.2); “implicit easing” must occur through visible governance proposals. PCIM cannot replicate countercyclical fiscal–monetary coordination; the “pushing on a string” problem in deep recession exists for protocols too—this is functional division, not theoretical failure.

MMT refined: real constraint is inflation—does protocol discipline ask the wrong question? Wray stresses that for monetarily sovereign states, real constraints are real resources and inflation, not account balances; government debt is a reserve-adjustment tool; job guarantees can be fiscally led without traditional financing constraints²¹. Fullwiler supplements from operational reality of central bank–Treasury: government spending creates reserves, taxation destroys reserves, bond issuance adjusts reserve balances—precise at double-entry level, not deriving “deficits harmless” or “inflation never comes”²². Bell earlier noted that at the operational level taxation and bonds cannot “finance” spending (government must spend first to create reserves to recycle), but can and must recycle liquidity to maintain price stability—MMT’s dispute with mainstream economics is therefore not over accounting identities but who should identify and execute inflation constraints⁵. Sargent and Wallace as early as 1981 noted that when fiscal deficits persist while the central bank tries to cooperate with low rates, long-term inflation pressure rebounds—“unpleasant monetarist arithmetic”²³; Kydland and Prescott’s “dynamic inconsistency” shows that even with central-bank commitment to low inflation, political cycles may force optimal plans to deviate *ex post*²⁴. These lines do not negate MMT’s operational description but imply: without reliable fiscal discipline and central-bank independence, monetary sovereignty alone does not guarantee price stability—Wray also admits MMT policy space presupposes floating exchange rates, domestic-currency debt, reliable tax base; missing any, the proposition should be narrowed²¹. Kelton’s popular *The Deficit Myth* vulgarizes MMT policy lists²⁵ but does not solve how fast “inflation constraint” becomes crisis in weak institutional environments. Leeper (1991) formalizes this tension in fiscal–monetary regime theory: price-stability equilibrium requires policies mutually matched on active/passive dimensions—if fiscal expands actively while monetary passively cooperates with low rates, Sargent–Wallace inflation consequences necessarily appear in equilibrium; Woodford (1996) gives parallel debt–price-stability conditions from public-debt dynamics²⁶. Thus MMT’s operational description and NK’s 2% welfare argument reduce to one proposition: macro stability is a multi-tool joint problem; no single anchor (tax, LOLR, inflation target, fiscal space) suffices to derive permanent monopoly mint prerogative—only that where anchors remain strong, the protocol path is marginal supplement, not retail-

layer full replacement. This book's response: MMT has partial truth in accounting identities under floating rates and domestic-currency debt but cannot be universalized—Turkey, Argentina, Venezuela and similar cases show weak tax bases, capital flight, and political pressure can quickly turn “inflation constraint” from abstract curve to real crisis; MMT policy advice lacks replicable institutional guardrails in high-inflation democracies. The protocol path does not answer “how to achieve full employment” but “when fiscal-monetary boundaries erode, can exit-capable, verifiable pricing and store-of-value options exist.” Protocols cannot replace redistributive politics; popularization expands participation and audit, not automatic welfare states.

The four academic defense lines above, together with strongest rebuttals—Terra/UST death spiral, liquidation cascades and oracle failure, governance capture, DeFi collateral thresholds and MEV discrimination, over-optimistic “competitive money is already happening”—are answered item by item elsewhere in the book (including Clements' s three algorithmic requirements, Ahmed et al. reserve-disclosure paradox, Auer et al. DeFi Terra cases and mechanism test points). The book's thesis can be summarized as transfer of constraint carriers toward verifiable rules, not claiming full replacement of tax anchor, lender of last resort, 2% welfare function, or MMT macro space; boundaries—crisis liquidity, thin-market peg, governance capture, marginal-corridor penetration to retail, reserve-disclosure paradox, three-layer BTG contention—require stress data, Ma et al. (2023)-style stablecoin flow panels, and cross-border adoption empirics, not roadmap presumption alone.

If CBDC closes programmability, it may strengthen the state anchor rather than weaken it—the popularization path must co-evolve with regulation; one cannot assume unilateral technological victory. Adoption in Venezuela, Argentina, and cross-border remittance corridors shows alternatives are tried first where anchors fail, not starting from New York supermarket checkout counters.

Sovereign currency in emerging markets and high-inflation economies follows another logic. In economies with sound rule of law and strong monetary discipline, the four pillars above are relatively firm; but where inflation long ran out of control, central-bank independence suffered political interference, and cross-border capital flows were strictly controlled, fiat's store-of-value anchoring is greatly weakened. Historical cases such as Argentina, Zimbabwe, and Venezuela show that when fiat's store-of-value function collapses, people vote with their feet, choosing dollarization or any available alternative store of value. According to several on-chain analytics firms, stablecoin per-capita usage intensity and retail adoption rank globally among the highest in these scenes (note: precise “penetration rates” are hard to certify due to differing statistical definitions and difficulty mapping on-chain addresses to real users—here a directional judgment, not precise measurement)²⁷—Eichengreen, Gupta & Masucci (2023) IMF working paper and World Bank (2023) remittance brief also record rising stablecoin cross-border payment adoption in high-inflation corridors, with regulatory arbitrage and reserve-transparency risks amplifying in parallel²⁷. Bullmann, Klemm & Pinna (2019), in pre-Terra-collapse ECB research, classified stablecoins along issuance accountability, decentralized responsibility, and collateral and noted systematic trade-offs between algorithmic “innovation” and peg capacity—marginal-corridor adoption must be read with Gadzinski et al. (2024) co-instability panels: in Terra/LUNA shocks algorithmic types were main shock receivers; fiat-collateralized and crypto-overcollateralized CDP types were relatively more resilient—one cannot extrapolate “monopoly has yielded” from single-chain TVL. Motivation is less technological superiority than more urgent need for substitutes. Real landing of the popularization narrative often does not start where institutions are soundest but in gaps where existing systems are weakest, then spreads toward the mainstream.

Historically, no monetary unit built credibility from nothing—gold accumulated millennia of use convention; the dollar's international reserve status is sediment of decades of post-WWII geopolitics and economic power. Protocol tokens must prove utility in real commercial scenes, stability under real market stress, and resilience in

real institutional conflict. This credibility accumulation cannot be replaced by technology manifestos or whitepapers—only by time and experience.

Section 3 CBDC: The Reverse Expansion of Digital Sovereignty

When analyzing challenge and challenged relations, one dimension is often oversimplified: the state can also actively adopt technology, not merely stand as a static challenged party. Global central-bank digital currency (CBDC) rollout is a systematic attempt to embed monetary sovereignty in digital infrastructure.

Technically, CBDC has two basic forms. Retail CBDC faces the public directly—each citizen can hold a digital account at the central bank; wholesale CBDC is limited to interbank use for interbank clearing. The former has stronger disintermediation effects on commercial banks; the latter mainly optimizes existing clearing architecture. Neither changes money’s liability nature: CBDC remains a liability on the central-bank balance sheet; the holder’s counterparty remains state credit.

To grasp CBDC’s strategic significance, look first at programmability. Technically, CBDC can carry execution conditions: directed spending constraints (subsidies usable only for specified categories), expiry dates (stimulating consumption not saving), automatic tax withholding (eliminating filing friction). Niepelt (2024) states the core tension in the How column: can programmable retail CBDC draw a line between “payment infrastructure” and “fiscal directed tool”²⁸—consistent with Bindseil’s “payment CBDC” emphasis in Chapter 10, Section 8. Bindseil and Panetta (2021) further operationalize this tension as tiered privacy: small offline anonymous, large online auditable—along with holding caps and waterfall mechanisms in digital-euro legislative drafts as control devices²⁹. Keister and Monnet (2022), from financial stability, add that CBDC availability reduces banks’ normal maturity mismatch; crisis migration speed to CBDC itself becomes a regulatory observable signal—net effect depends on design; one cannot a priori judge “CBDC necessarily worsens runs”²⁹. Such programmability raises micro policy-transmission efficiency and macro monetary–fiscal coordination; yet it triggers deep political-economy controversy: when money itself becomes a pipeline for policy execution, monetary neutrality collapses; when every consumption detail can be tracked, privacy boundaries face structural challenge.

For the protocol ecosystem, CBDC rollout is complex. On one hand it may absorb part of “fiat digitization” demand, compressing stablecoin market space; on the other, CBDC with open-interface design may become a compliant channel between public-chain ecosystems and traditional finance—BIS Project Dunbar and mBridge and other multilateral wholesale CBDC experiments already explore cross-border settlement linkage²⁸. In any case, CBDC means the future of digital currency is not only the decentralized-protocol route—the state chose to strengthen rather than abandon monetary sovereignty in digital space. This is strategic background that must be faced when discussing protocol collaboration and state monopoly.

Section 4 Open Source, Multi-Client, and Censorship-Resistant Technical Logic

Discussing state monopoly’s resilience, one cannot ignore the antifragile structure protocol collaboration builds at the technical layer. This structure was not designed for confrontation, yet its result is: shutting down a single server cannot equal destroying an open-source rule set.

Distinguish “service” from “protocol” first. Traditional financial infrastructure depends on specific institutions operating specific services: SWIFT is a messaging system jointly operated by member banks; cutting a country’s SWIFT access paralyzes its cross-border clearing. Bitcoin differs: its rules are encoded in open-source software anyone can run; nodes span dozens of jurisdictions globally. Shutting all nodes within one country, the global network still runs; users in the shut country, if they can reach the network, can still verify ledger state.

Ethereum goes further. Its “multi-client” design requires key network infrastructure to be implemented by multiple independent teams in different programming languages. Geth, Nethermind, Besu, and Erigon are all Ethereum execution-layer clients; vulnerability or compromise of any single client is insufficient to make the whole network err. This design philosophy analogizes to diversified clearing in finance—any single-point failure has redundant coverage. Multi-node, multi-jurisdiction deployment raises the real cost of shutdown, forcing regulators to act on protocols indirectly by affecting participants (exchanges, wallet providers, banking channels) rather than directly closing the protocol. Historically, offshore financial centers already show capital and rule arbitrage space always exists in sovereign-boundary gaps. Protocol globality and programmability digitally amplify such arbitrage space.

Censorship resistance must honestly face its double edge. Money launderers, fraudsters, and ransomware attackers use the same infrastructure, often earliest and most active adopters. Protocol design that bypasses this reality in the name of “technological neutrality” is cognitively dishonest. True monetary popularization must incorporate governance and compliance interfaces at the protocol layer: freezable addresses (in permissioned deployments), auditable issuance records, standardized linkage to off-chain identity systems. These designs are not betrayal of popularization but necessary conditions to enter mainstream society. Protocols refusing compliance interfaces will long be isolated at the competitive periphery by mainstream finance.

In Chapter 23 of *The Denationalization of Money*, “Preventing the Recurrence of Government Interference,” Mr. Hayek asks: even with open private competition, the state may restore monopoly through re-monopolization, forced legal tender, or regulatory capture—competitive schemes must preset institutional structures resistant to re-monopolization³⁰. Open-source code, multi-client redundancy, and cross-jurisdiction node deployment partly answer this concern: shutting one server does not destroy rules, but does not equal Hayek-style competition gaining legal guarantee—regulation can still pressure indirectly through exchanges, banking channels, and stablecoin reserve review. Popularization here should be understood as marginal practice of dispersing state monopoly mint prerogative, not declaring the state has exited monetary affairs; the protocol side must treat compliance interfaces, audit trails, and governance timelocks as anti-re-monopolization engineering components, coordinated with gradual transition paths.

Section 5 Mint Prerogative Can Be Dispersed; Money Endures

The tension between institutional foundations above and the protocol path, here, echoes the book’s central thesis head and tail. Central thesis: money will not be abolished; state monopoly mint prerogative will—when value bookkeeping, transfer, and issuance rules can be publicly verified at low cost, discipline against abuse shifts from “issuer reputation” to “protocol verifiable rules.” Mr. Hayek wanted to change “who prints”; this book wants to change “what discipline rests on”; they overlap but differ. This judgment’s key: necessary conditions give the lower bound of constraint-carrier transfer; sufficient conditions give the upper bound of erosion of state monopoly mint prerogative legitimacy—between them lies the marginal evolutionary trajectory this book describes, not prophecy of overnight fiat replacement. In summary: when $N1 \wedge N2 \wedge N3$ persistently hold in target scenes, constraint carriers complete transfer from reputation to verifiable rules; when the conjunction stably holds in high-friction scenes and participants can create, hold, and compose value units at lower cost than traditional licensing paths, state monopoly mint prerogative legitimacy faces observable sustained erosion—the latter is sufficient condition; its converse does not hold.

“The Popularization of Money” neither means universal enrichment, nor cancels division of labor, nor is an unregulated free market in money; it describes state monopoly mint prerogative dispersed, constrained, and audibly substituted under open protocols—competitive minting can still exist but no longer under sovereign

exclusive monopoly. Medium of exchange and unit of account endure; state money, central banks, and legal order will coexist for the foreseeable period. Popularization is marginal expansion and institutional competition, not “monetary death” in the medium-of-exchange sense. The subtitle’s “value in direct flow” must be institutionally reread: what is abolished is state monopoly mint prerogative, not exchange and clearing itself, nor all minting activity.

Necessary conditions. If abuse discipline is to shift from “issuer reputation” to “protocol verifiable rules,” three observable conditions must hold simultaneously—missing any, constraint carriers cannot complete transfer and “popularization” degenerates into slogan or centralized packaging: (N1) rules public—issuance, collateral, supply caps, and other key parameters readable by any third party; (N2) execution verifiable—on-chain state or equivalent audit interfaces let “whether rules are obeyed” be independently checked without fully trusting issuer self-report; (N3) transfer routable—value units can flow at low cost on interoperability infrastructure (VTP, IBC, cross-chain bridges, etc.), making competition and exit technically possible. $N1 \wedge N2 \wedge N3$ are necessary for constraint-carrier transfer; satisfying one or two alone is insufficient for institutional migration from reputation to rules—long failure of any condition narrows the proposition to “supplementary tool in specific scenes.”

Sufficient conditions. When $N1 \wedge N2 \wedge N3$ stably hold in high-friction scenes—cross-border clearing, supply-chain private-domain settlement, machine-agent payments—and participants can create, hold, and compose value units at lower cost than traditional licensing paths, monopoly mint prerogative legitimacy faces sustained challenge: multi-subject competitive issuance, auditable rules, and multi-unit coexistence become observable institutional directions. What is described is an equilibrium trajectory of marginal erosion, not prophecy of overnight fiat replacement. Mr. Hayek wanted to change “who prints” (private bank competition); this book wants to change “what discipline rests on” (from trusted institution to verifiable rules). They overlap but differ: protocol competitive units are rule suites and interoperability standards, not bank licenses; state money may not disappear, but pluralization of subjects creating and governing money is itself institutional qualitative change³¹.

In Chapter 9 of *The Denationalization of Money*, Mr. Hayek concretizes bank competition as issuance competition among distinguishable named currencies: homonymous, freely interchangeable notes if issued in parallel by many parties let no one be responsible for quantity and value; competition must occur among units with transparent rules and accountable issuers, issuers trading continued existence for purchasing-power stability³². Clearinghouse networks, option clauses, and reputation discipline form its micro-mechanism—Selgin (1988) ch. 2–4 and Rockoff (1992) U.S. state comparisons show discipline can partly endogenize in discount clearing, yet likewise depends on bond-collateral rules and whether authentication costs are controllable; Kroszner (1996) cautions extrapolation³³. This book moves competitive units up to protocol rule suites—whether heterogeneous rule competition equals homogeneous multi-issuer sharing the same PCIM rules as Hayek-style competition remains theoretically open.

Under this proposition, “participation” includes holder, user, creator (designing and issuing new value representations), and governor (voting on protocol evolution). Structural threshold decline means: without central-bank license, without full reliance on political endorsement, without limitation to a single jurisdiction, one can attempt new value-unit design—success or failure still filtered by market, rule of law, and code; failure costs borne by participants. Popularization is not equalization: protocols lower institutional thresholds to attempt, not guarantees of success.

The proposition must accept empirical rebuttal. If open value-transfer protocols and competitive public-domain issuance mechanisms (such as PCIM) cannot maintain necessary conditions under liquidity crisis, governance capture, or regulatory squeeze, the proposition should narrow to “supplementary tool in specific

scenes” rather than “general path of dispersing state monopoly mint prerogative.” Conversely, if they persistently lower participation cost and constrain implicit expropriation in high-friction scenes, “money will not be abolished; state monopoly mint prerogative will” gains support as an institutional-direction proposition. Expanded participation opportunity and equal outcomes are different matters; popularization includes the possibility of universal failure—institutional cost participation freedom must bear.

Configuration-efficiency gains from dispersed mint prerogative lie in using dispersed knowledge: a single issuer cannot know which assets deserve collateral, which incentives suit which scene—protocol-layer plural issuance lets local knowledge aggregate through markets into effective value-tool choice. This finds new concretization in monetary affairs for classical economics’ claim that price mechanisms transmit knowledge: planners remain in the all-knowing position; rule openness encodes dispersed knowledge into market outcomes.

Section 6 Protocol Collaboration as a New Institutional Form

From institutional economics, protocol collaboration is not merely technical architecture but a new social coordination mechanism. Traditional institutions have two extremes: market (decentralized decisions, price signals) and hierarchy (centralized decisions, command control). Modern finance evolved between them: commercial banks are market subjects, but deposit insurance and lender of last resort are hierarchical intervention; central banks are policy institutions but influence market prices through open-market operations.

Protocol collaboration introduces a third coordination prototype: rules embedded in code, execution by the network, evolution through governance proposals and on-chain voting. This form is neither pure market (protocol rules are not set by real-time prices) nor pure hierarchy (no single subject holds final veto). It closer resembles constitutional order—a set of foundational rules collectively recognized by participants, permitting market behavior within the rule frame, requiring collective deliberation when rules revise.

This quasi-constitutional order’ s advantage is predictability and auditability. All participants know rules in advance; past records are checkable; rule revision requires explicit procedure. This contrasts with traditional monetary systems where “monetary policy depends on committee judgment”—though committee decisions have professional-division advantages, process non-verifiability remains critics’ attack point. Weaknesses exist too. On-chain governance has low participation, large-holder vote manipulation, uneven proposal quality. Code bugs may void carefully designed rules. Governance-crisis cases reveal on-chain democracy’ s slow reaction to emergencies. Quasi-constitutional robustness ultimately depends on participant quality and governance-culture maturity, not technology alone.

Protocol collaboration as institutional form is at an early stage of any major institutional arrangement—similar to seventeenth-century joint-stock companies: idea present, but legal framework and commercial practice need generations of trial and adjustment. Acknowledging this stage is honest attitude toward this new form—neither overpraise nor belittle.

Within this frame, governance quality not governance form determines protocol collaboration’ s actual value. Long-low on-chain vote rates are ecosystem-wide: most token holders ignore governance proposals; those actually deciding are often few active nodes and large holders. Thus “decentralized governance” in practice diverges significantly from theoretical design. Improvement requires incentive design: make governance participation cost lower than benefit, make non-participation cost visible. Timelocks, delegated voting (liquid democracy), specialized governance tokens—all explore engineering paths to raise governance participation quality. PCIM circulation-tier referenda turn “when to relax mint output rate” from back-room team parameters into automatic proposal on tier trigger plus community vote—failed upgrade leaves discipline unchanged; crisis tightening separately uses referendum track to raise collateral requirements—concretizing quasi-constitutional

order in monetary discipline: rule revision must be procedurally visible, not silent relaxation when circulation hits a tier.

A more fundamental question: should protocol governance' s "decentralization" be a goal or a means? If decentralization' s purpose is preventing single-subject abuse, a protocol actually dominated by few technical elites may be formally decentralized yet substantively highly concentrated. True popularization must achieve dispersion in participation structure, not only technical architecture—a long-term issue for protocol designers and ecosystem participants.

Section 7 Long-Term Coexistence: The Contours of a Realistic Equilibrium

Synthesizing the above, one can sketch a relatively realistic long-term equilibrium contour rather than overly optimistic or pessimistic extremes.

State monetary monopoly will not collapse wholesale but will be marginally eroded continuously. Fiat' s dominance in tax anchoring, public spending, and retail daily transactions will long persist; protocol tokens and stablecoins will gradually expand share in cross-border settlement, open-ecosystem internal pricing, inter-institutional clearing, and incentive design in specific scenes. This is functional-division evolution, not zero-sum replacement. Boundaries among functional layers will float dynamically with technological evolution, regulatory adjustment, and market game—not freeze at one moment.

CBDC rollout will partly compress decentralized stablecoin markets but may also provide new compliant channels for protocol ecosystems. Differentiated national regulation will spawn regulatory arbitrage and jurisdiction competition—this competition will not disappear, only find new forms. Protocol collaboration networks' value will first appear in institutionally weak scenes: high-friction cross-border remittance corridors, emerging markets with high domestic-currency inflation, international trade settlement lacking effective legal protection. These are gaps where existing financial infrastructure under-serves—and where new protocols best prove practical value.

The popularization of money is a continuous process, not arrival at some endpoint: protocols improve technological boundaries, regulation updates institutional boundaries, users redraw market boundaries with action. Protocol collaboration and state monopoly form complex institutional co-evolution, not simple challenge and challenged—the state strengthens sovereignty in digital space (CBDC) while protocol ecosystems accumulate interoperable value in jurisdictional gaps. This co-evolution is designed by no single subject but jointly shaped by participants in game and collaboration.

注释与引用

1. Knapp, 1905/1924, *The State Theory of Money*, English ed. ch. 1: money is first the state-established "unit of account" (*money is a creature of law / Zahlungsmittel*); value comes from the state' s ability to define payment obligations. Internet Archive: <https://archive.org/details/statetheoryofmon030559mbp> ↩
2. Innes, 1914, "The Credit Theory of Money," *Banking Law Journal* 31(12): "money is not a thing but a law"; 1913 "What is Money?" same journal 30(5). Collection: <https://www.community-exchange.org/docs/Innes/> ↩
3. Goodhart, Charles A. E. "The two concepts of money: implications for the analysis of optimal currency areas." *European Journal of Economics and Economic Policies: Intervention* 1(1), 2004, pp. 9–23 (orig. *Economic Journal* 108(447), 1998; chartalism and metallism long coexist; debate on institutional division). <https://doi.org/10.1111/1468-0297.00291> ↩ ↗²

4. Wray, 2012, *Modern Money Theory*, ch. 2: taxation creates demand for domestic currency; spend-first, finance-later fiscal cycle. Palgrave Macmillan 2012 ed. ↩
5. Bell, Stephanie A. "Can Taxes and Bonds Finance Government Spending?" *Journal of Economic Issues* 34(2), June 2000, pp. 603–620: taxation and bonds cannot operationally "finance" spending but must recycle reserves to maintain price stability; dialog with Wray (2012) ch. 2 tax-driven demand. <https://doi.org/10.1080/00213624.2000.11506379> ↩ ↗²
6. Bagehot, 1873, *Lombard Street*, ch. 2, 7: "lend freely at a penalty rate on good banking securities" (*lend freely at a penalty rate on good banking securities*). Project Gutenberg: <https://www.gutenberg.org/ebooks/4359> ↩
7. Goodhart, Charles A. E. *The Evolution of Central Banks: A Natural History*. MIT Press, 1988. Ch. 4–5 (lender of last resort as ex post recognized invention; joint with moral hazard and deposit insurance). MIT Press 1988 ed. ↩
8. Mehrling, Perry. *The New Lombard Street: How the Fed Became the Dealer of Last Resort*. Princeton University Press, 2011. Ch. 1 (from Bagehot lender of last resort to post-2008 "dealer of last resort"; shadow-banking liquidity). Princeton 2011 ed. ↩
9. MakerDAO community, March 12, 2020 "Black Thursday Post Mortem": ETH crash triggered liquidation spiral, zero-price auctions, DAI premium; same day Fed launched large-scale repo and QE. Forum: <https://forum.makerdao.com/> ↩
10. Brunnermeier, Markus K., and Dirk Niepelt. "On the Equivalence of Private and Public Money." *Journal of Monetary Economics* 106, 2020, pp. 27–41 (equilibrium equivalence of private and public money under appropriate fiscal–central-bank division; contrasts with chartalist ontology). <https://doi.org/10.1016/j.jmoneco.2019.10.006> ↩
11. Calomiris, Charles W. "Deposit Insurance: Lessons from the Record." *Economic Perspectives*, Federal Reserve Bank of Chicago, May/June 1989, pp. 2–41 (lender of last resort, deposit insurance, moral hazard; cost side of monopoly mint prerogative "rationality"). <https://www.chicagofed.org/publications/economic-perspectives/1989/05> ↩
12. Woodford, 2003, *Interest and Prices*, ch. 6 (pp. 235–280, welfare foundation of moderate positive inflation under nominal rigidity), ch. 7 (pp. 281–330, zero lower bound ELB constraint). Princeton University Press 2003 ed. ↩
13. Rotemberg, Julio J., and Michael Woodford. "An Optimization-Based Econometric Framework for the Evaluation of Monetary Policy." In *NBER Macroeconomics Annual 1997*, vol. 12, MIT Press, 1997, pp. 297–346 (New Keynesian DSGE policy evaluation; estimable FIT welfare foundation). <https://doi.org/10.1086/654340> ↩
14. Galí, 2015, *Monetary Policy, Inflation, and the Business Cycle*, 2nd ed., ch. 8 (pp. 145–180, New Keynesian optimal monetary policy), ch. 15 (pp. 320–340, flexible inflation targeting and discretion–commitment trade-off). Princeton University Press 2015 ed. ↩
15. Clarida, Richard, Jordi Galí, and Mark Gertler. "The Science of Monetary Policy: A New Keynesian Perspective." *Journal of Economic Literature* 37(4), December 1999, pp. 1661–1707 (New Keynesian reaction function and FIT theoretical foundation). <https://doi.org/10.1257/jel.37.4.1661> ↩
16. Bernanke, Ben S., et al. *Inflation Targeting: Lessons from the International Experience*. Princeton University Press, 1999. Ch. 1–2 (2% anchor, expectation management, transparent communication institutionalization). Princeton 1999 ed. ↩
17. Eggertsson, Gauti B., and Michael Woodford. "The Zero Bound on Interest Rates and Optimal Monetary Policy." *Brookings Papers on Economic Activity*, 2003(1), pp. 139–211 (zero lower bound and optimal average inflation). <https://doi.org/10.1353/eca.2003.0010> ↩
18. Blanchard, Olivier, Giovanni Dell’Ariccia, and Paolo Mauro. "Rethinking Macroeconomic Policy." IMF Staff Discussion Note SDN/10/03, February 12, 2010, pp. 1–18 (post-crisis reflection: whether 2% remains optimal under ELB; welfare trade-off of higher inflation target). <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Rethinking-Macroeconomic-Policy-22486> ↩
19. Schmitt-Grohé, Stephanie, and Martín Uribe. "Liquidity Traps and Letter of Last Resort Policies." *American Economic Review* 104(5), May 2014, pp. 110–115 (under ELB optimal policy must tolerate inflation overshoot or fiscal coordination; dialog with Eggertsson–Woodford 2003). <https://doi.org/10.1257/aer.104.5.110> ↩
20. Sargent, Thomas J. *The Conquest of American Inflation*. Princeton University Press, 1999. Ch. 2–3 (Volcker tightening, rational expectations, institutional maintenance cost of inflation anchoring). Princeton 1999 ed. ↩
21. Wray, 2012, *ibid.*, ch. 5–6: fiscal space under floating exchange rates and domestic-currency debt; real constraints are inflation and resource availability, not account balances. ↩ ↗²

22. Fullwiler, Scott T. "Modern Money Theory and Interrelations between the Treasury and the Central Bank: An Operational and Institutional Analysis." Levy Economics Institute Working Paper No. 855, 2016, pp. 1–35 (MMT operational description: spending creates reserves, tax destroys, bonds adjust; does not derive deficits harmless). <https://www.levyinstitute.org/publications/modern-money-theory-and-interrelations-between-the-treasury-and-the-central-bank> ↩
23. Sargent, Thomas J., and Neil Wallace. "Some Unpleasant Monetarist Arithmetic." *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1981, pp. 1–17 (long-term inflation consequences when fiscal deficits persist with central-bank low-rate cooperation). <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ↩
24. Kydland, Finn E., and Edward C. Prescott. "Rules Rather than Discretion: The Inconsistency of Optimal Plans." *Journal of Political Economy* 85(3), June 1977, pp. 473–491 (dynamic inconsistency; time-inconsistency of discretionary frameworks). <https://doi.org/10.1086/260580> ↩
25. Kelton, Stephanie. *The Deficit Myth*. PublicAffairs, 2020 (popular MMT; contrast with Wray 2012 academic ed.). ↩
26. Leeper, Eric M. "Equilibria under 'active' and 'passive' monetary and fiscal policies." *Journal of Monetary Economics* 27(1), 1991, pp. 129–147 (fiscal/monetary active–passive combinations and price-stability equilibrium); Woodford, Michael. "Control of the Public Debt: A Requirement for Price Stability?" In *NBER Macroeconomics Annual 1996*, vol. 11, MIT Press, 1996, pp. 143–169 (public-debt dynamics and price stability; dialog with Sargent–Wallace 1981). [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ; <https://doi.org/10.1086/654291> ↩
27. Chainalysis (2024), *The 2024 Geography of Cryptocurrency Report*: stablecoin receipt intensity in high-inflation and emerging markets; Gorton & Zhang (2022), *University of Chicago Law Review* 89(1), pp. 1–52: dollar stablecoins as on-chain dollar extension—empirics and regulatory frame; Eichengreen, Gupta & Masucci (2023), IMF WP 23/110: emerging-market corridor stablecoin cross-border payments; Aquilina et al. (2023), BIS Bulletin No. 73: stablecoin market structure and run contagion; World Bank (2023), *Migration and Development Brief* 37, Box 1.2: remittance corridors and crypto adoption; Bullmann, Dirk, Jonas Klemm, and Andrea Pinna (2019), ECB OP 230: three-dimensional stablecoin classification and algorithmic peg trade-offs; Gadzinski, Gregory, et al. (2024), "Break a peg! A study of stablecoin co-instability," *International Review of Financial Analysis* 96, 103608: Terra/LUNA co-instability and CDP resilience contrast. <https://www.bis.org/publ/bisbull73.htm> ; <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf> ; <https://doi.org/10.1016/j.irfa.2024.103608> ↩ ↩²
28. Niepelt (2024), *CBDC: Whence, Why, What, and How*, MIT Press, ch. 5–6 (programmable CBDC and fiscal–central-bank division); Bindseil (2024), ECB OP 322, §5–6 (payment CBDC); BIS Innovation Hub, "Project Dunbar" (2022 PoC) and "Project mBridge" (2024 MVP): multilateral wholesale CBDC cross-border settlement. <https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm> ↩ ↩²
29. Bindseil, Ulrich, Fabio Panetta, and Ignacio Terol (2021), "Central Bank Digital Currency: Functional Scope, Pricing and Controls," ECB Occasional Paper Series 286, §3–4 (tiered privacy, functional scope, waterfall mechanism); Keister, Todd, and Cyril Monnet (2022), "Central Bank Digital Currency: Stability and Information," *Journal of Economic Dynamics and Control* 142, 104501 (OFR WP 22-04, §1–2, 3.3: maturity-mismatch decline and run signals); Auer, Cornelli & Frost (2022), "CBDC and financial stability," *BIS Quarterly Review* March 2022, pp. 55–68 (account-type default traceability). <https://ssrn.com/abstract=3975939> ; https://www.financialresearch.gov/working-papers/files/OFRwp-22-04_central-bank-digital-currency.pdf ; https://www.bis.org/publ/qtrpdf/r_qt2203e.htm ↩ ↩²
30. Mr. Hayek, 1976, *The Denationalization of Money*, ch. 23 "Preventing the Recurrence of Government Interference": competitive money must preset institutional arrangements preventing government re-monopolization. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
31. Selgin, George, and Lawrence H. White, "How Would the Invisible Hand Handle Money?" *Journal of Economic Literature* 32(4), December 1994, pp. 1718–1749 (competitive issuance, clearinghouses, option clauses); White, Lawrence H., "Competitive Payments Systems and the Unit of Account," *AER* 84(3), 1994, pp. 699–712 (protocol-layer competitive units vs. bank-personality historical contrast); Calomiris, Charles W., "Deposit Insurance: Lessons from the Record," *Economic Perspectives*, Federal Reserve Bank of Chicago, May/June 1989, pp. 2–41 (free-banking debate counter-side: lender-of-last-resort shadow). ↩
32. Mr. Hayek, 1976, *The Denationalization of Money*, ch. 9 "Competition Between Banks Issuing Different Currencies," pp. 49–51: competition among distinguishable named currencies superior to monopoly; homogenous interchangeable tokens if competitively issued let no one control quantity responsibly; issuers must trade purchasing-power stability for survival, failure loses business. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩

33. Selgin, George, *The Theory of Free Banking* (1988), ch. 2–4, pp. 25–78 (competitive issuance, discount clearing); Rockoff, Hugh, "Lessons from the American Experience with Free Banking," in Dowd (ed.), *The Experience of Free Banking* (1992), ch. 4, pp. 73–86 (state institutional differences); Kroszner, Randall S., "Free Banking: The Scottish Experience as a Model for Emerging Economies?" *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31 (cautious extrapolation).

↩

§ 25 Paths of Transition

Protocol collaboration and state monetary monopoly will long coexist with marginal erosion—from a fiat-only landscape toward a layered ecosystem of multiple protocols and multiple units, what is the path? Transition spans decades, not an overnight technical revolution; cross-border settlement, supply-chain private-domain networks, machine-readable tokens, and autonomous-program settlement are scenes where marginal substitution lands first. Below we discuss starting points, mechanisms, constraints, and the respective roles of enterprises, individuals, regulators, and autonomous systems.

Section 1 The Logic of Marginal Substitution

Estonia's e-Residency and digital-identity system and Singapore's Project Guardian tokenization trials represent states gradually absorbing on-chain settlement through "sandbox" approaches rather than abandoning fiat monopoly overnight.

To discuss transition, one must first drop the imagination of "overnight full replacement." Fiat will not declare death on some day; central banks will not close after a parliamentary resolution. Real transition occurs at the margin, accumulating gradual functional substitution into structural change.

The mechanism of marginal substitution: in scenes where the existing fiat system serves weakly or costs are high, new protocol tools embed step by step, accumulating users and liquidity, forming local positive network effects, then expanding substitution scope. This logic contrasts with Knapp-style tax anchoring: tax obligations create rigid domestic-currency demand in domestic retail and wage flows¹, but cross-border B2B, open-ecosystem internal settlement, and store-of-value demand at high-inflation margins are not equally bound by a single sovereign unit of account—marginal substitution therefore enters first where anchors fail or friction is highest, not from supermarket checkout counters. Brunnermeier and Niepelt (2020) give testable institutional premises for this path: parallel units must be convertible to the public anchor when needed and fiscal-central-bank division must recycle liquidity overflow—missing any condition, parallel currencies degenerate into non-interconvertible IOUs, not an expandable settlement layer². Canzoneri, Cumby, and Diba (2001) further note that even with parallel units, the price level long-term must align with fiscal solvency—Sims (1994) fiscal theory of the price level (FTPL) writes the same constraint into a minimal model: under active fiscal paths, inflation is equilibrium outlet for debt dilution, not mere technical choice³. Cross-border corridors and high-inflation store-of-value scenes often precisely activate the C-money layer where tax bases are weak or anchors fail—this does not negate Knapp-style tax demand but shows Goodhart-style M-money / C-money division boundaries drift with anchor strength. Fullwiler's description of MMT operational reality mirrors here: when tax bases are weak, capital flight, or political pressure erodes the fiscal anchor, the "spend first, recycle later" cycle can still operate at the operational level, but inflation constraints quickly surface in Sargent-Wallace-style rebound—stablecoin penetration in high-inflation economies is partly result of dual failure of tax and fiscal anchors, not mere tech fashion⁴. Sargent-Wallace's "unpleasant monetarist arithmetic" reminds from another angle: when fiscal deficits persist while the central bank cooperates with low rates, the domestic anchor itself loosens through inflation rebound⁵—marginal substitution leads in weak institutions; in developed economies where anchors remain strong, retail-layer substitution must be measured on generational scales.

This book does not advocate overnight abolition of domestic legal tender, but accumulation of marginal substitution outside scenes where fiat anchors remain strong—spiritually aligned with Mr. Hayek's revised-edition Chapter 1 "A Realistic Proposal" that European countries mutually open currency and banking competition

—superior to issuing a common European currency—as a gradual first step in transition rhythm; competitive units shift from bank-personality competition to verifiable protocol-rule competition; state money and central banks will still coexist for the foreseeable period.

One must simultaneously distinguish transition strategy from institutional endpoint: Mr. Hayek long held that for competitive discipline to fully operate, forced legal tender must ultimately be removed so bad money can be rapidly eliminated by markets—this is a directional premise, not a day-one operations manual. In Chapter 22 Mr. Hayek also requires one-time release of competitive freedom at transition, avoiding gradual monopoly residue (pp. 121–122)—this book takes a more conservative marginal-substitution path on political feasibility, using warnings of old fiat rapidly depreciating under competitive pressure to show: even without overnight abolition of legal tender, monopoly currency runaway depreciation must be prevented⁶. From this follows a transition path: marginal substitution and sandbox adoption first; legal tender and tax anchors in domestic retail left to generational evolution; not using “gradualism” to evade competitive discipline’s logical endpoint, nor using “endpoint” to skip transition’s contractual continuity and political feasibility—compliance interfaces, audit trails, and governance timelocks must advance together with anti-re-monopolization design.

The most typical entry scene is cross-border payment. Traditional cross-border remittance relies on correspondent-bank systems, passing multiple intermediaries, multiple currency conversions, multi-day settlement cycles—fees weigh especially heavily on low-income remittance populations; global average remittance rates long exceeded 5%, some corridors over 10%. Stablecoin remittance actual fees are usually below 1%, settlement in minutes. Marginal substitution in this scene has already occurred in parts of Latin America, Southeast Asia, and Africa—not hypothetical.

Supply-chain internal settlement is another gradual path. Prepayment management, receivables financing, cross-border trade settlement—in these scenes settlement via VRC-11 private-domain stablecoins or dedicated enterprise tokens can reduce reliance on bank intermediaries, speed capital turnover, and reduce exchange-rate volatility interfering with contract performance. Internal settlement between large manufacturers and tier-one suppliers historically had precedents in commercial paper and internal bookkeeping as non-fiat tools; VRC-11-class tools merely move this practice onto programmable on-chain rails, giving stronger auditability and cross-organizational interoperability.

On-chain bond and equity financing is a more structurally significant gradual path. Real-world asset (RWA) tokenization already places sovereign bond fund shares, corporate bonds, and real-estate equity on public chains at growing scale. Traditional institutional investors’ gradual acceptance of on-chain assets will push clearing and settlement infrastructure toward hybrid mode—not either-or replacement. Hybrid mode means on-chain clearing and off-chain legal enforcement in parallel; smart contracts handle automation; traditional legal frameworks handle disputes and exceptions.

Cumulative effect of marginal substitution must not be underestimated. Historically commercial-bank deposit money replaced metallic coin and credit cards replaced cash—all through marginal substitution completing structural change. Looking back decades, change is startling; living inside, each year’s change is tiny. Transition participants need sufficient time horizon not to be misled by short-term noise before marginal substitution accumulates into structural change.

Section 2 Legal Clarity: The Biggest Bottleneck of Transition

If technology is already in place, the single largest factor constraining transition progress is severe lack of legal clarity. This judgment rests on many practical cases: countless valuable protocol projects stalled, migrated, or closed because they could not obtain reliable answers about their legal status.

Legal ambiguity exists at multiple levels. Product classification comes first: whether a token is security, commodity, currency, or payment instrument—different countries and regulators give different answers, standards changing anytime. Classification uncertainty directly affects compliance obligations: if deemed security, disclosure, investor suitability, broker licensing apply; if payment instrument, AML, stored-value management, payment-clearing rules apply. Building business under unsettled classification is construction on ground that may shift anytime. Read alongside tax anchoring: tax obligations force holding domestic currency but do not prohibit choosing other verifiable pricing units in contracts, cross-border, and permitted private-domain layers—EU MiCA separates “electronic money tokens” and “asset-referenced tokens,” drawing parallel rule space outside the legal-tender circle; transition’s legal task is therefore executable classification and liability chains for protocol units in off-anchor scenes, not abolishing tax anchors⁷.

Cross-border jurisdiction is the second layer of conflict. Public-chain protocols run globally; code deployment location, user location, and asset location often separate. Traditional jurisdictional principles depend on geographic nexus, yet public-chain assets are inherently geographically fuzzy. When a company registered in one country operates an Ethereum smart contract serving users in another, which country’s law applies? Current answers vary by event type, with mutually contradictory precedents. This ambiguity spawns much regulatory arbitrage—practitioners do not actively seek gray zones but passively adapt in rule vacuum.

Liability assignment is the third blank. Smart contracts execute automatically by code logic; when results cause user loss due to code bugs, external oracle manipulation, or parameter error, who bears legal liability? Contract deployer? Governance-token holders? Protocol foundation? Existing legal frameworks are almost blank here, preventing reliable legal opinions and blocking institutional investors needing clear liability chains.

Two paths improve legal clarity. Active path: industry and regulators jointly push specialized legislation or interpretive guidance clarifying classification, liability, and compliance routes—EU MiCA and some countries’ digital-asset frameworks are efforts in this direction, each with limits. Passive path: accumulation of judicial cases forming de facto precedent—long cycle, high cost, very unfriendly to practitioners trapped in legal gray. Either path, raised legal clarity is necessary precondition for accelerated transition. Ambiguity breeds opportunism and sudden heavy regulatory strikes—neither favors long-term sustainable ecosystem adoption.

Protocol designers can actively create conditions for legal clarity rather than passively wait for regulatory frameworks. Concrete measures: built-in compliance interfaces at protocol layer (KYC/AML whitelists, freezable addresses, on-chain audit logs) letting regulators fulfill obligations without overturning protocol architecture; active sandbox cooperation accumulating regulator-recognized compliant operation records in controlled environments; participation in industry standard-setting pushing self-regulatory frameworks regulators can reference. These investments raise compliance cost short-term but are the most effective path to accumulate institutional credibility before regulatory frameworks crystallize.

Legal clarity also closely relates to jurisdiction choice. Some economies have made clear, friendly digital-asset regulatory frameworks competitive strategy to attract innovative firms, providing operable compliance anchors for industry. This competition materially affects global regulatory landscape: when innovative firms can operate compliantly in more permissive jurisdictions, economies with harsh or fuzzy frameworks face pressure of talent and capital outflow. This is institutional dividend of regulatory competition for protocol ecosystems and external pressure pushing economies to clarify regulatory stance.

Section 3 The Role and Strategy of Enterprises in Transition

Enterprises are the most action-capable middle layer in transition. They combine flexible technology adoption with resources to drive institutional change; their collective behavior will deeply affect transition speed and form.

Large multinationals' core challenge is rising complexity of multi-currency financial management. When employee wages must be paid in multiple fiat currencies, raw-material procurement involves emerging-market currencies, and digital-business revenue settles in stablecoins, traditional single bookkeeping-currency systems begin to friction. Demand for multi-currency treasury tools—including on-chain settlement accounts, automated exchange routing, multi-chain liquidity management—is real and being filled by protocol-layer firms focused on enterprise financial infrastructure. Tool maturity driven by this demand will in turn lower SME adoption thresholds.

Supply-chain scenes have special meaning for SMEs. When tier-one suppliers adopt on-chain settlement, downstream SMEs are often passively drawn in. Passive involvement is both pressure and opportunity: pressure to quickly learn new tools; opportunity that on-chain settlement can greatly improve SMEs' receivables capital occupation—traditional bill financing has long cycles and high cost, while on-chain receivables can approach real-time confirmation and transfer, directly improving SME cash-flow structure. For cash-strapped SMEs, this improvement's practical value may exceed remittance fee savings.

Mid-size enterprise strategy usually chooses: mature SaaS hosted services (outsourcing technical complexity) or self-built on-chain financial infrastructure (stronger customization but higher operational risk). Current ecosystem maturity favors the former: self-build cost high, security risk large, technical talent scarce; hosted SaaS choice requires careful review of provider compliance status and asset-security mechanisms, avoiding transferring rather than eliminating risk.

At corporate governance level, issues requiring serious attention: accounting treatment, tax filing, and disclosure standards for on-chain assets are not unified. Whether to measure on-chain assets at fair value or historical cost differs across accounting frameworks. This is not merely technical but board risk judgment under incomplete information. Early entrants can build internal frameworks with auditors and tax advisors, accumulating practical experience before standards unify—this first-mover advantage becomes institutional competitive barrier when rules finally clarify.

Section 4 The Real Thresholds for Individual Participants

"The popularization of money" is often understood as personal-empowerment slogan, yet honest assessment of real thresholds is equally indispensable. Popularization means participation opportunity opens to individuals, not that participation risk is automatically eliminated.

Individuals' first challenge is private-key management. "Not your keys, not your coins" holds technically, yet practice demands far higher security awareness and discipline than most ordinary users' habits. Cold-wallet mnemonic management, multisig setup and recovery, hardware-wallet use—each exceeds ordinary banking operations. Forgotten mnemonics, hardware failure, phishing attacks have caused permanent asset loss for many users. Much loss falls on ordinary participants who should benefit most from popularization—they most need lower thresholds yet often first become victims of security gaps.

Financial-literacy requirements also rise. Reading a protocol's tokenomics document requires grasping supply curves, incentive mechanisms, governance structure; evaluating stablecoin collateral adequacy requires first distinguishing stable-mechanism spectra (Maker-style liquidation auctions vs. VRC-10/11, see glossary). These demands are hard even for well-educated finance practitioners; for broad ordinary users they are significant cognitive burden. Education gaps do not auto-close with technology; financial-literacy improvement speed is often hidden bottleneck constraining social spread of new financial tools, impact sometimes exceeding technical maturity itself.

Fraud and information asymmetry are another real constraint. Protocol-token markets have high information asymmetry: insiders know project progress far better than external investors; on-chain data are public yet interpretation needs professional skill. Rug pulls, structural Ponzi yield protocols, fake audit reports are widespread fraud forms in current ecosystems. Technology can raise transparency but cannot eliminate individual differences in information discrimination.

Popularization's advance must accompany effective consumer protection and investor education. Consumer protection and investor education are institutional guarantees for sustainable popularization—not contradictory to popularization ideals. An ecosystem where participants suffer large-scale loss will ultimately lose claimed inclusive value through credibility collapse. For individuals, participation premise is minimum literacy to identify risk, not being blinded by tech-optimist narrative.

Custody-service choice and evaluation is among individuals' highest-weight decisions. For ordinary users unwilling to bear self-custody complexity, centralized exchanges and custodians offer lower-threshold paths but introduce counterparty risk—historical failures of leading exchanges causing user asset loss are real cost of this risk. Evaluating custodian audit reports, proof-of-reserve mechanisms, insurance coverage, and regulatory compliance is basic judgment ability when choosing custody paths.

From broader social view, financial-literacy improvement is not only personal responsibility but public good. If basic education does not incorporate digital-asset fundamentals into financial-literacy curricula, as protocol ecosystems penetrate, vulnerable groups (elderly, low-income, financially illiterate) will bear higher risk exposure than early adopters—popularization's distributional effect may backfire. This social dimension often ignored in popularization policy discussion must enter policymakers' view parallel to regulatory design. If popularization benefits only few with cognitive advantage, it is merely old financial elitism in new tech clothing, contrary to claimed inclusive value.

Section 5 Evolving Division of Labor with CBDC

In transition, CBDC's role is an unavoidable variable. Most likely division: CBDC covers public payments, social-benefit disbursement, personal daily retail consumption; public-chain stablecoins and protocol tokens cover cross-border settlement, open-ecosystem internal pricing, inter-institutional clearing, and asset-liquidity management. The two are not diametrically opposed but play comparative advantages in different scenes. CBDC has state-credit endorsement and legal coercion but is limited in composability and cross-chain interoperability by sovereign boundaries; protocol stablecoins have technical advantage in programmability and global interoperability but lack sovereign credit as backstop. Must also bound: CBDC and most compliant stablecoins anchor sovereign fiat units—digital extension or mirror of state money, not heterogeneous private competitive new units in Hayek's sense—their value discipline still ties to domestic central bank and fiscal, not independent purchasing-power competition.

Realizing this division depends on policy choice. If regulators allow stablecoins and CBDC to cooperate on interoperability interfaces—for example CBDC entering and exiting stablecoin liquidity pools as optional collateral—the two systems can complement. Conversely, if regulators use CBDC rollout to comprehensively suppress private stablecoins, division will solidify coercively, sacrificing innovative-ecosystem diversity. Bindseil (2024) stresses: retail CBDC if designed as “payment type”—low interest, holding caps, two-tier operation—functions closer to cash extension than full replacement of bank intermediation; lender of last resort remains on central-bank balance sheet; CBDC does not change Bagehot-style crisis-function division, only retail payment carrier⁸. Historically coercively solidified monetary arrangements often form new inefficiencies long-term, spawning substitute demand in institutional gaps.

Internationally, interoperability among multiple CBDCs is larger institutional arrangement. Cross-border CBDC platform pilots—projects such as mBridge—aim to lower cross-border settlement cost and time within sovereign-currency frameworks. If successful, they partly substitute current cross-border stablecoin remittance markets; yet they also demonstrate comparative advantage of on-chain real-time clearing in cost and timeliness, accumulating credibility for the whole protocol ecosystem.

An unexpected cognitive spillover: CBDC popularization may accelerate public understanding and acceptance of on-chain financial tools. Ordinary users paying with CBDC already know digital wallets and chained-ledger basics; jumping from that entry to public-chain assets is far smaller cognitive leap than from zero. State CBDC promotion objectively lowers protocol ecosystem user-education cost—a rare two-way spillover in bilateral game.

CBDC versus protocol stablecoin competition is ultimately competition over user experience and ecosystem convenience, not only technical route. If CBDC user experience is smooth enough and scene coverage broad enough, it may become many users' first digital-value entry; if public-chain stablecoins keep advantage in composability and cross-chain function, they will keep accumulating users in scenes CBDC cannot serve efficiently. Final division will gradually appear through users' daily choices via market mechanism, not one policy document's final word.

Section 6 Regulatory Coordination: From Unilateral Jurisdiction to Multilateral Frameworks

One institutional premise of transition is major economies' regulatory frameworks gradually evolving toward multilateral coordination. Currently major jurisdictions differ significantly on protocol tokens, stablecoins, and exchanges, often making unilateral decisions affecting global markets. This regulatory fragmentation creates much arbitrage space and accumulates institutional friction.

Ideal multilateral regulatory frameworks should rest on several consensus principles: mutually recognized disclosure standards (whether on-chain data can satisfy certain disclosure obligations), cross-border enforcement data-sharing mechanisms (tracing illicit on-chain asset flows), minimum-common-denominator alignment on regulatory classification (at least preliminary consensus on “what is stablecoin, what is security-type token”). These principles are not unreachable ideals but coordination modes with precedent in traditional financial regulation—Basel Accord alignment on bank capital adequacy offers reference institutional path.

Financial Stability Board, Bank for International Settlements, and Basel Committee already have series of working papers and policy frameworks in this direction, but from principle consensus to member-state legislation usually needs years or a decade. In this transition, industry self-regulatory bodies and technical standardization institutions actually fill coordination gaps, using technical standards instead of legal treaties—this itself concretizes protocol collaboration as institutional form. Ethereum Foundation, Cosmos IBC standards committee, and similar bodies lack legal coercion yet shape participant behavior boundaries through widely adopted technical standards.

Regulatory coordination speed ultimately depends on financial-stability risk magnitude. When protocol ecosystem scale is large enough that systemic risk spillover touches traditional finance, political motivation for regulator coordination truly heats. This is a paradoxical logic: ecosystem must first matter enough for coordination to occur; yet coordination absence constrains sustainable growth. Breaking this cycle requires pioneer countries' frameworks clear enough to serve institutional templates for others—as dollar clearing system provided de facto anchor for global financial regulatory coordination.

Section 7 The Time Scale of Gradual Migration

Technical full readiness does not mean immediate migration. Historical monetary-institution change offers useful time-scale reference: Bretton Woods establishment and collapse each took about twenty years; euro introduction from treaty to banknote circulation exceeded ten years; credit-card social spread from invention to mainstream coverage likewise took decades. Institution-change speed is constrained by the slowest link—often not technology but supporting legal frameworks, user habit, and political consensus.

Synthesizing legal-clarity improvement speed, user-education accumulation, CBDC introduction rhythm, and institutional adoption scale effects, one can sketch an evidence-based gradual transition picture: current decade, cross-border settlement and inter-institutional clearing are fastest protocol-tool penetration scenes—scale effects and infrastructure maturity will lay foundation in this phase; middle decade, as accounting/tax standards clarify and custody infrastructure matures, enterprise-finance on-chain share will gradually rise; long two-to-three decades, user cognition and regulatory generational evolution will bring on-chain value tools’ social penetration toward today’ s credit-card magnitude.

This time scale means transition is long-horizon institutional trend, not speculative short-track bet. Practitioners need neither wait for “perfect regulatory certainty” before acting (that moment may never come) nor presume protocols will replace all fiat within five years (almost certainly not). Real window: build real business in marginal-substitution scenes, layout on gradually clarifying legal tracks, build migratable capability on mature technical standards. This is “protocol thinking” in the time dimension: rules first, execution stepwise, evolution continuous.

Time-scale estimates require humility. Technology’ s social spread often shows nonlinearity: long slow penetration then possible rapid jump triggered by key event—as smartphone spread in some regions seemed overnight though base technology accumulated over a decade. For protocol ecosystems, trigger might be major economy issuing clear regulatory framework, major institution adopting on-chain settlement, or major traditional-finance turmoil suddenly highlighting alternative value. Transition timetable uncertainty must be accommodated with strategic elasticity, not replaced by precise timing prediction for directional judgment. Grasp direction, accommodate uncertainty, accumulate real capability at the margin—most resilient strategic posture in transition.

If transition has an endpoint, that endpoint is qualitative change in participation structure—more subjects can create and use value units under transparent rules—not some monetary institutional form declaring final victory.

One dimension often overlooked in gradual transition discussion is human-capital distribution. Protocol ecosystem expansion depends on many practitioners with compound skills: understanding financial-product economic logic, mastering blockchain engineering, designing compliant product architecture under legal frameworks. Such compound talent is extremely scarce globally—a practical bottleneck constraining ecosystem expansion speed. University curricula have not systematically incorporated cross-training in protocol economics and smart-contract engineering; traditional financial institutions’ internal training only beginning to include on-chain assets. Human-capital accumulation cycles are generational—reason transition progress still constrained by talent supply after technology readiness.

Compared with technical-route debate, standardized quality of ecosystem infrastructure will be more foundational factor determining transition speed. Wallet experience, on-chain data readability, contract-interaction safety—these user-facing engineering problems need sustained product and developer investment. Whitepaper ideal design becomes popularization only when ordinary people dare use the product—not stuck in

geek circles. Transition speed often depends on whether this user-experience layer can keep pace with protocol evolution.

注释与引用

1. Knapp, 1905/1924, *The State Theory of Money*, ch. 1; Wray, 2012, *Modern Money Theory*, ch. 2—tax anchor's binding force in domestic scenes. See Chapter 24, Section 2 footnotes ¹⁵. ↩ ↩²
2. Brunnermeier, Markus K., and Dirk Niepelt. "On the Equivalence of Private and Public Money." *Journal of Monetary Economics* 106, 2020, pp. 27–41 (equivalence three conditions: convertibility, fiscal recycling, shared unit of account; institutional premise of marginal substitution). <https://doi.org/10.1016/j.jmoneco.2019.10.006> ↩
3. Canzoneri, Matthew B., Robert E. Cumby, and Behzad Diba. "Is the Price Level Determined by the Needs of Fiscal Solvency?" *American Economic Review* 91(5), December 2001, pp. 1221–1238 (fiscal solvency anchor; read with Leeper 1991, Sargent–Wallace 1981); Sims, Christopher A. "A Simple Model for Study of the Determination of the Price Level and the Interaction of Monetary and Fiscal Policy." *Economic Theory* 4(3), 1994, pp. 381–399 (FTPL minimal model). <https://doi.org/10.1257/aer.91.5.1221> ; <https://doi.org/10.1007/BF01215355> ↩
4. Fullwiler (2016), Levy WP 855, pp. 1–35: MMT operational reality—spending creates reserves, tax recycles, bonds adjust; when tax base weak operational cycle can still run but inflation constraint surfaces in Sargent–Wallace-style rebound. Dialog with ch24 §2 MMT refined version. <https://www.levyinstitute.org/publications/modern-money-theory-and-interrelations-between-the-treasury-and-the-central-bank> ↩
5. Sargent & Wallace (1981), "Some Unpleasant Monetarist Arithmetic," *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1981, pp. 1–17: high deficits with low-rate fiscal cooperation must eventually pay in higher inflation; cross-ref Chapter 24 Section 2 MMT dialog and high-inflation stablecoin penetration (ch24 §2). <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic> ↩ ↩²
6. Mr. Hayek, 1976, *The Denationalization of Money*, ch. 22 "The Problem of Transition," pp. 121–122: new order must grant competitive freedom at once; gradual opening tends to fail; must prevent old monopoly currency accelerating depreciation during displacement. Revised preface (1978) and p. 83 of main text also admit monetary scheme "probably be practicable only as part of a much more far-reaching change in our political institutions"—contrast with this book's marginal-substitution path and long coexistence of state money. Revised ed. ch. 1 "A Realistic Proposal" European mutual currency competition see ch04 §7 [²⁵]. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
7. EU Regulation (EU) 2023/1114 (MiCA), Arts. 3–6 (electronic money token EMT / asset-referenced token ART classification); Goodhart (1998) M-money / C-money division. MiCA full text: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> ↩
8. Bindseil, Ulrich. *Central Bank Digital Currency: Considerations, Projects, Outlook*. ECB Occasional Paper Series 322, 2024, §5–6 (payment CBDC, holding caps and two-tier operation; LOLR remains central-bank layer). <https://www.ecb.europa.eu/press/pdf/scpops/ecb.op322~5822218919.en.pdf> ↩

§ 26 The Long-Term Vision of the Value Internet

Transition paths depict process; the value internet is direction. Internet pioneers in 1993 could not foresee today's social media and e-commerce—the contour of direction is discernible, detail cannot be preset. The following synthesizes the long-term vision of the value internet and frankly faces risks and uncertainties that cannot be eliminated.

Section 1 The Infrastructure Logic of the Value Internet

The Bank for International Settlements' 2023 report notes that tokenized deposits and wholesale CBDCs may coexist with the SWIFT messaging network at the cross-border settlement layer—the BIS Committee on Payments and Market Infrastructures' 2020 cross-border payments roadmap lists compliance interfaces, FX liquidity, and interoperability standards as harder bottlenecks than raw technical speed alone¹². The value-internet vision presents long-term coexistence and competition among multi-layer infrastructure, not overnight replacement.

The value internet can be read alongside the internet: first see how the transport layer drives cost toward zero, then distinguish where value transfer differs.

The internet's core contribution is to drive the cost of transmitting information toward zero and, through standardized protocols (TCP/IP, HTTP, SMTP), give that low-cost transmission global interoperability. The historical significance of standardized protocols lies in separating application-layer competition from base-layer collaboration. Email providers compete fiercely, yet all mail interoperates via SMTP; websites compete for traffic, yet all pages are reachable via HTTP. Open standards at the base layer are the institutional precondition for diverse innovation at the application layer. This architectural choice—open base, competing applications—released the densest wave of information-industry innovation in human history over the past thirty years.

The value internet seeks a similar cost reduction and standardization for value transfer. VTP parallels TCP/IP, supplying addressing and routing standards for value transmission; IBC and VRC parallel HTTP and email format standards, defining cross-chain communication and asset-interface specifications. Openverse is designed as a Layer 0 value-exchange layer—coordinating consensus, final-settlement anchoring, and cross-domain routing so various Layer 1 networks can connect, rather than forming a closed hub-subnet LAN. If this system matures, cost of value transfer among different chains and asset types should approach information-transmission cost, not today's cross-border fees often running to several percentage points. A deeper effect is composability: when value units can be arbitrarily combined and programmed like packets, contract logic can seamlessly link flows across asset types, compressing the cost of building complex financial products from months of legal negotiation to deployment of a few lines of code.

Yet value and information differ in one core attribute: value transfer is zero-sum (if I transfer to you, I have less); information copying is not (if I send to you, I still have it). This difference means value-internet infrastructure must solve problems the information internet need not: prevention of double spending, confirmation of final settlement state, and global consistency of value state. Nakamoto, in the Bitcoin white paper, reduced this to the requirement that “pure electronic cash” prevent double spending without relying on a trusted third party³; Szabo, from the angle of “social scalability,” argued that verifiable rules lower the marginal trust cost of stranger collaboration—on-chain ledgers are the engineering of that logic in the monetary domain⁴. This is the fundamental contribution of blockchain technology: through distributed consensus, it maintains global

consistency of value state without a central trust institution. It is infrastructure innovation of the same order as TCP/IP, though its social diffusion remains early.

Section 2 The Form of Multi-Center Equilibrium

The evolutionary direction of monetary institutions tends toward a layered, multi-center, composable ecological equilibrium—not convergence to “one optimal currency wins.”

Multi-center means that in different economic scenes and institutional environments, different value units play their comparative advantages, and can convert among themselves via protocol bridges and liquidity pools. This resonates deeply with actual historical monetary systems: any theory prophecy of a “single optimal currency” is broken in reality by monetary hierarchy and scene dependence—the gold-standard era had layers of domestic currency, foreign exchange, commercial bills, and bank deposits; the fiat era has M0, M1, M2; the value-internet era further expands the number of layers and degree of customization, and at the public layer overlays reserve-circulation division: fixed-supply Bitgold as world reserve collateral, a few VRC-10 Bitcurrencies as dynamic global circulation media—not two hundred-plus mappings listed in parallel equality. Menger, in “On the Origin of Money,” stressed that money emerges from barter as the most saleable good, rather than becoming money only after state decree⁵; Schumpeter, in *History of Economic Analysis*, read the succession of bank notes, deposit money, and central-bank institutions as credit instruments repeatedly creatively destroying old layers⁶.

During the transition period, fiat and CBDC remain dominant in domestic retail: Knapp-style tax anchoring, Bagehot-style last-resort capacity, and completeness of the legal framework are their institutional advantages⁷. The Woodford–Galí New Keynesian framework further supplies welfare justification for roughly 2% inflation targets: under nominal rigidity, moderate inflation buffers relative-price adjustment and eases zero lower bound risk—Clarida–Galí–Gertler formalized this logic as the “science” of central-bank reaction functions⁸, and Bernanke et al. bound the 2% anchor with expectation management as institutional consensus across many countries⁹. Brunnermeier and Niepelt’s equivalence theorem hints that even when the unit of account is state-defined, privately verifiable units can bear parallel functions under appropriate institutions—requiring convertibility, fiscal recycling, and a shared unit of account; missing any one, parallel units remain confined to marginal corridors¹⁰. Multi-center equilibrium is therefore closer to a functional-division equilibrium than a utopian fantasy. Public-service payments, social-welfare disbursement, and everyday personal retail consumption will, for the foreseeable transition period, long remain primarily priced and settled in fiat; protocol tokens do not seek to fully substitute this layer in macro-stabilizer function, but supply verifiable parallel discipline in cross-border, open-ecosystem, and high-friction scenes.

In the long-term vision, VRC-10 Bitcurrencies mapped to domestic currencies can run in parallel with sovereign fiat: domestic wages and tax may still use domestic currency; cross-border and on-chain default to public-layer mapping units—the two linked by instant conversion and dual-track accounting—Bitcurrency is an on-chain extension of sovereign domestic currency, not a simple “foreign-currency invasion.” The global C-money circulation layer tends toward convergence on a few public Bitcurrencies and the BTG reserve layer; mappings of monetary-policy miscreants lose public-layer standing first in parallel competition; convergence does not preset specific countries—it depends on liquidity, compliance, and international friendliness, with no timetable commitment.

Cross-border stablecoins and public-layer currencies gradually gain importance in cross-border settlement and internal pricing within open ecosystems. Cross-border scenes are where existing fiat friction is highest and where protocol tools’ comparative advantage is most pronounced. If public-layer currencies (e.g. Bitcurrency as envisaged in VRC-10/PCIM white papers, dynamic tiers of excess collateral, upper tier roughly $C_0 \approx 161.8\%$) can

maintain long-term collateral adequacy and governance robustness, they will play the functional role of international clearing currency in the most liquid cross-chain ecosystems globally—must be layered against VRC-11 Privcurrency’s low collateral (61.8%): the latter serves permitted trade circles and cannot apply public-layer > 100% standards, and is not the global main circulation medium. As the Eurodollar market once spawned a deregulated dollar settlement system outside sovereign borders¹¹, the global protocol stablecoin market will spawn similar functional substitutes within protocol boundaries—but main circulation media concentrate in a few mappings, not two hundred units competing equally.

Enterprise tokens and asset tokens perform customized settlement in private and vertical scenes. Internal supply-chain settlement, industry-specific receivable circulation, and liquidity management of real-estate rights—these scenes’ needs are highly customized; a universal currency cannot satisfy all parameters; protocol standards supply customizable templates so vertical scenes can achieve differentiated functions under standard interfaces.

Time vouchers and service tokens open new forms of value representation in professional services and the gig economy. Tokenizing professional time, specific commitments, and service-delivery horizons is an important direction extending the monetary spectrum from “things” to “promises.” Liquidity and market depth of such assets are extremely limited today, but as internet-native value representations, their long-term potential cannot be ignored.

Multi-center equilibrium does not realize itself automatically. It depends on effective exchange-rate discovery among layers, adequate cross-layer liquidity, and robust bridge security. Systemic failure at any link can trap or evaporate value at one layer. Multi-center is not a decentralized utopia; it is a dynamic order sustained jointly by protocol standards, market liquidity, and regulatory frameworks—its robustness depends on continuous investment by participants and overall ecosystem health.

Multi-center equilibrium also involves a deep paradox of competition and cooperation: value layers both compete for users and liquidity and must depend on one another to maintain overall liquidity depth. The relation between fiat and protocol stablecoins typifies this paradox: stablecoin anchor value comes from fiat, yet stablecoin expansion also erodes fiat use scenes. Such coopetition is not rare in mature markets—competition between commercial banks and money-market funds, between bank credit and bond markets, follows similar logic. The key is whether this competition is constrained by sufficiently clear rules so that it raises overall efficiency without disorderly competition breeding systemic risk.

From investors’ and users’ perspective, multi-center equilibrium means “what to hold” is no longer a single answer. Wisdom in asset allocation will increasingly depend on understanding comparative advantage and risk characteristics across layered value units, rather than simply “all fiat” or “all Bitcoin.” This shift in cognition is itself popularization of money at the individual level: every participant must bear more information-processing responsibility in exchange for more participation opportunity.

Section 3 Open Issues in Technological Evolution

The long-term vision of the value internet partly depends on whether underlying technology can keep breaking current key bottlenecks. Frank assessment of these bottlenecks is a necessary part of any serious outlook.

Scalability is the most persistent technical challenge. Mainstream public chains’ transactions per second still lag significantly behind traditional payment-clearing infrastructure. Layer 2 has greatly raised throughput in some ecosystems, but bank-grade throughput while preserving decentralization and security is not fully solved.

The “trilemma”—decentralization, security, scalability hard to achieve together—is the core engineering constraint protocol designers face. For the value internet to cover global retail payment, unit cost must be further compressed without sacrificing core attributes.

Balance between privacy and transparency is another open issue. Public-chain ledger transparency aids compliance and audit but threatens personal privacy and corporate commercial secrets. Zero-knowledge proof (ZKP) technology supplies a cryptographic path to “prove a condition is satisfied without exposing the information itself,” potentially reconciling privacy protection and auditability. Today ZKP computation cost is high and engineering complexity limits broad deployment; as technology matures and hardware accelerates, this constraint may gradually ease.

The oracle problem—the mechanism by which on-chain contracts obtain reliable off-chain world information—remains a fragile link connecting real assets and on-chain protocols. Price-feed manipulation and centralized data-source risk have repeatedly caused major protocol losses. Decentralized oracle networks mitigate centralized risk to some extent, but long-term robustness of their incentive mechanisms still awaits market test.

On a longer horizon, potential threat of quantum computing to current cryptographic assumptions deserves attention. Existing public chains rely heavily on elliptic-curve digital signature algorithms whose security rests on the assumption that quantum computers cannot efficiently break the underlying mathematical hardness. If practical quantum computers mature within coming decades, existing public chains must complete systematic migration of cryptographic algorithms—a far-reaching infrastructure upgrade whose time pressure and execution difficulty are not trivial. Research on related post-quantum cryptographic standards is advancing, but from standard establishment to full ecosystem migration, historically similar infrastructure upgrades often exceed ten years.

Technical bottlenecks do not negate the direction of the value internet, but they supply important real-world calibration to any optimistic timetable. Infrastructure maturity is never a single exponential line; it advances unevenly between technical breakthrough and engineering accumulation.

Section 4 Major Risks That Must Be Faced

A long-term outlook that writes only possibility lacks half its prudence. Smart-contract bugs, governance capture, cyclical collateral collapse, regulatory shocks, and fraud must be set alongside optimistic narrative—mechanism detail is developed further in Tokenomics and public-currency chapters.

Smart-contract bugs can cause loss even after audit and formal verification; upgradeable contracts introduce new trust assumptions. Bearing large-scale ordinary-user savings on this infrastructure remains a proposition to be argued.

Governance capture, when holdings concentrate, can reduce on-chain governance to oligarchic decision; timelocks and split-track governance can only mitigate, not fully eliminate capital’s concentration into power.

Cyclical collateral collapse: when crypto collateral plunges, MakerDAO-style CDPs with L may trigger liquidation cascades (March 2020 “Black Thursday”); VRC-10/PCIM sets no L/W —stress paths shift to redemption runs + reserve depletion—avoiding auction cascades, not eliminating extreme-market risk. VRC-11 private layer additionally overlays off-chain redemption squeezes. Algorithmic stablecoins (Terra/UST) are a third failure type—not to be conflated with excess-collateral CDPs.

Regulatory shocks—unilateral bans or enforcement actions—can reshape ecosystem landscape in the short term; they must be included as basic assumptions in long-term planning.

Fraud and social harm amplify fraud scale in early high-value, low-friction ecosystems; regulatory enforcement, industry self-discipline, and user education must combine—technology alone cannot solve.

Facing these risks sets a realistic baseline for optimistic narrative. Realization of popularization depends on sustained response across technology, institutions, and society—not on technology’s natural gift.

Section 5 A New Monetary Constitution

From a macro-historical perspective, every major transformation of monetary institutions accompanies some form of “monetary constitution”—a foundational institutional arrangement about who may issue money, under what rules, and what rights holders possess.

The gold standard was one monetary constitution: gold reserves as hard constraint limited issuers’ discretionary room to expand money and gave holders explicit right to convert into physical commodity. Eichengreen, in *Globalizing Capital*, traces how nineteenth-century gold standard relied on convertibility promises and capital flows rather than a single world central bank¹². Bretton Woods was another monetary constitution: key currency as anchor, other currencies pegged, forming a hierarchical global monetary order—Triffin, in the 1950s, pointed out that the dollar simultaneously bore domestic liquidity and international reserve functions; intrinsic tension would eventually erode anchor credibility¹³. Post-1971 fiat is a monetary constitution substituting central-bank credit and political promise for physical anchoring—its core is independence commitment and inflation targeting, using institutional norms to constrain unverifiable political behavior. Keynes, in *A Tract on Monetary Reform*, already distinguished monetary policy’s short-term temptation from long-term credibility cost: “In the long run we are all dead” is not abandonment of rules but warning that discretion faces tension between short-term employment and long-term currency value¹⁴. The New Keynesian tradition represented by Woodford and Galí supplies the most rigorous welfare argument for this constitution to date: flexible inflation targeting incorporates employment gaps in the reaction function, claiming distributional concerns are internalized in discretionary framework¹⁵. Ball, Mankiw, and Romer (1988) earlier wove nominal rigidity + rational-expectations anchoring into the “New Keynesian synthesis”—Walsh (2017) textbook operationalizes it as teachable, estimable policy-analysis language¹⁶. Friedman, in *A Program for Monetary Stability* (1960), offered another middle path of “rules over discretion”: impose $k\%$ fixed money growth on existing central banks rather than open private competitive money—rules still executed by committee; third parties cannot independently verify compliance¹⁷. On-chain PCIM’s C_0 , mint/redemption rules, and oracle circuit breakers are logically closer to “rules hardened in code + state-machine execution + third-party verifiability”—same anti-discretion spectrum as $k\%$, differing in executing subject (central bank vs protocol) and whether ELB countercyclical function can be borne (Eggertsson & Woodford 2003; Schmitt-Grohé & Uribe 2014)¹⁸. Blanchard et al., post-crisis, ask: if the zero lower bound becomes a recurring constraint, is 2% average inflation still the optimal constitutional parameter—a higher target leaves room to cut policy rates but at cost of steady-state welfare and expectation-management cost¹⁹; Schmitt-Grohé and Uribe show that under ELB, optimal policy often must tolerate temporary inflation overshoot or rely on fiscal coordination—constitution is therefore multi-tool joint; no single fixed rule (whether central-bank reaction function or on-chain collateral parameters) can bear macro stability alone²⁰. Kydland and Prescott’s “dynamic inconsistency” warns from the reverse: even with optimal discretionary rules designed, political cycles may still force central banks to deviate ex post from commitment²¹—precisely the incentive problem protocol paths try to answer with on-chain verifiable parameters. Each monetary constitution has rationality under its historical conditions and intrinsic fragility—2021–2022 inflation de-anchoring shows that even with optimal theory support, discretionary frameworks can still misjudge; fiscal space as MMT describes can also run out of control in weak tax-base, high-inflation polities.

The emergence of protocol tokens explores a new prototype monetary constitution: code-written rules substitute part of political promise; publicly verifiable execution substitutes part of reliance on institutional trust. Revision of issuance rules still requires some form of collective consent; protocol ecosystems still operate within sovereign legal frameworks—this is partial transformation of monetary trust mechanism: from “trust institutions, cannot independently verify their behavior” to “trust rules, can independently verify execution.”

This transformation is not necessarily superior to current institutions. Rule rigidity may lack necessary flexibility in crisis response; code verifiability depends on users’ technical literacy; decentralized governance may bring decision inefficiency. But it supplies a new possibility: outside fiat institutions, another trust mechanism exists whose strengths and weaknesses complement rather than fully replace existing institutions.

A new monetary constitution will not end the old system at its center with a block of code; it will more likely experiment at the old system’s margins in protocol form with new constraint mechanisms and participation structures, accumulate credibility, and await recognition and adoption by broader social forces. This needs time, repeated failure and improvement, and gradual legal adaptation. Constitutional history is like this—it rarely decreed on one day; it slowly condenses into consensus through long political practice.

Section 6 Policy, Enterprise, and the Individual

Whether policymakers, enterprise operators, technology developers, or ordinary savers and investors, evolution of monetary institutions touches immediate interests; all must judge and act under incomplete information.

For policymakers, the most important principle is reversibility. In domains of rapid technological change, choose policy frameworks that can update with new information rather than prematurely solidifying rules that may prove wrong. Historical lessons in monetary regulation repeatedly show: overly harsh early control often drives innovation offshore rather than eliminating it; when innovation grows wild in regulatory vacuum, remedial regulation’s cost and risk rise sharply. Prioritize verifiable information-disclosure standards rather than premature product classification of new assets; calibrate carefully between suppressing systemic risk and preserving experimental space rather than leaning to either extreme.

For enterprise operators, treat on-chain protocol supply curves, collateral structures, and governance proposals as reading monetary products’ “new financial statements.” Technology-stack choice must weigh protocol long-term sustainability, not only current market heat—protocol-standard compatibility often determines whether today’s technical investment accumulates through ecosystem evolution or must be rebuilt. Early investment in compliant architecture for on-chain business is far cheaper than ex post remediation; early compliant architecture is also an important signal for institutional partners and regulatory trust.

For technology developers, compatibility with widely accepted protocol standards such as VRC and ERC, investment in formal verification and security audit, is the most important foundational investment in long-term product value. Technically clever but isolated protocols are often replaced by compatible standards in ecosystem evolution; technology that can embed in existing interoperability networks can convert developers’ intellectual accumulation into lasting ecosystem value.

For ordinary savers and investors, raised financial literacy is the most basic weapon for self-protection in the new monetary landscape. Mises, in *Human Action*, reminds that all market exchange ultimately rests on actors’ subjective judgment under uncertainty²²—understand issuance mechanism and collateral structure of held assets, identify risk assumptions behind high-yield promises, prioritize protocol products with high transparency

and complete audit records. Diversify custody; do not concentrate risk on a single exchange or single protocol. Systematic skepticism toward any “technically risk-free high yield” holds in every asset class.

Section 7 The Long Lens of Institutional Evolution

If one views the future of monetary institutions on a fifty-year rather than five-year horizon, a more robust judgment framework emerges.

Monetary institutions in any era are historical sediment of interaction among technological possibility, political structure, and social trust. Technology supplies the toolkit; politics sets use boundaries; social trust endows the toolkit monetary value. These three change at different speeds: technology fastest, measured in years; political structure in the middle, in decades; migration of social trust slowest, in generations.

The technological toolkit of protocol tokens has grown in little more than a decade from zero to supporting trillions of dollars in asset flow—a speed still rare in modern financial history. Yet rapid technological evolution has not automatically reconfigured political structure or triggered large-scale social-trust migration. This is the essential reason popularization is “in progress” not “completed.” Mr. Hayek, in Chapter 24 “The Long-Run Prospects,” foresaw: after competition weeds out failed experiments, the free world would coexist with several extensively used and very similar currencies—geographic dominance of currencies blurred, border zones overlapping—not single optimal currency winning all, nor disorderly fragmentation²³. Multi-center equilibrium aligns with this spirit but stresses more functional layering (division of labor between fiat/CBDC and protocol units) and rule verifiability as new dimensions of competition; state money’s dominance in tax-anchored scenes is also retained longer than in Mr. Hayek’s original scheme. Fifty years hence, which technologies prove foundational and which prove fleeting, cannot be asserted today. But the following trends carry high institutional inertia: programmable value will continue penetrating every link of financial contracts; on-chain transparency standards will become new benchmarks for asset information disclosure; protocolization of cross-border settlement will continue compressing traditional correspondent-banking share; individual participation in governance of value units will move from margin toward mainstream in some vertical scenes.

Historically, every new monetary tool, before mainstream social acceptance, underwent a long credibility-accumulation period. Paper money, across centuries of history, repeatedly faced trust crises and abuse, finally achieving relatively stable credibility anchoring under central-bank institutional framework²⁴. Protocol tokens are in early history—credibility accumulation has only begun, institutional framework is still groping, failure and success cases coexist. Noise of this early stage is the inevitable groping of major institutional innovation; it should not be misread as error of direction.

The long lens of institutional evolution also reveals an important comparative dimension: rather than treating protocol money as fiat substitute, treat it as a new member of humanity’s coordination toolkit. Mr. Hayek, in *Individualism and Economic Order*, characterized market order as spontaneous order—rules generated in dispersed interaction, not centrally blueprinted and decreed once²⁵. Humanity’s coordination tools keep expanding—from gift exchange within tribes, to regional commercial credit, to global bank clearing systems. Each expansion lowered friction cost of some transaction type and introduced new risk types. Protocol money is the latest chapter in this expansion sequence, not the final chapter. What it lowers is trust cost of certain value transfers—especially cross-border, cross-subject transfers without common judicial backing; new risks it introduces are code bugs, governance failure, and technical inaccessibility.

Under this long lens, the question “will the value internet succeed?” may ask in the wrong direction. A more accurate question is: in humanity’s coordination toolkit, in what form will programmable value-transmission

protocols be incorporated? Scope and depth of incorporation depend on whether they can continuously prove comparative advantage in real scenes and whether institutional systems can absorb their value while effectively managing their risk.

Section 8 Closing the Value Internet

Sections 1–7 of this chapter sketch value-internet infrastructure, multi-center form, technical bottlenecks, and policy roles. Global fiat mapping, minting as choice, bad money exiting, reserve–circulation division, and the book’s closing on money itself unfold in the last two chapters of Part VII (Chapters 27 and 28).

The following closes the main line of value internet and seigniorage institutional change as conclusion to Part VI through the first half of Part VII; the book’s popularization-of-money proposition closes in the final chapter, leaving farther open questions.

Seigniorage moved from lords’ mints into central-bank balance sheets over centuries; today it is partly moving into open-source repositories and smart contracts anyone can read. This process is unfinished and will not be declared complete at any moment—but it is clear enough to confirm its meaning within civilization’s coordinates.

Medium of exchange and measure of value endure; what protocolized competitive issuance erodes is state monopoly of seigniorage, not money itself, nor all minting participation—money will not be abolished; state monopoly of seigniorage will; the subtitle’s closing phrase “value in direct flow” must be read institutionally: we abolish state monopoly of seigniorage, not exchange and clearing itself. Marx, in Part I of Volume I of *Capital*, characterized the money form as inner unfolding of commodity exchange, not arbitrary pasting of exogenous symbols—medium-of-exchange function therefore has deep historical materiality²⁶. When bookkeeping, transfer, and issuance rules can be cheaply publicly inspected, discipline against abuse must rely on collateral ratios, mint and redemption rules, supply caps, and audit interfaces as protocol state third parties can independently verify—not institutional self-report—constraint carrier shifts from issuer reputation to protocol verifiable rules; Mr. Hayek wanted to change “who prints notes”; this book wants to change “what discipline rests on”²⁷. State money and protocol units will long coexist; popularization is marginal extension and institutional competition, not monetary extinction in the sense of medium of exchange—the state does not disappear, the central bank does not disappear, law does not disappear. Popularization is neither a technical promise that everyone gets rich nor an anarchist monetary utopia, but under publicly verifiable rules, diffusing participation in creation, holding, and governance of money and value networks from a few license oligarchs to any individual or organization willing to bear corresponding responsibility.

This does not mean technology automatically delivers justice; code bugs, governance capture, and regulatory shocks remain real costs—but the nature of the problem has changed: monopoly legitimacy must face auditable alternatives, not only another set of institutional promises. These propositions can be tested and refuted—if protocol collaboration continuously lowers participation cost and constrains implicit taxation in high-friction scenes, the evolutionary direction of multi-unit coexistence, auditable rules, and dispersed seigniorage gains support; if it fails comprehensively in systemic crisis, the proposition must be revised.

Monopoly legitimacy comes from real problems it solved under specific historical conditions: unified unit of account, last-resort provision, financial stability—Bagehot, Woodford, and MMT traditions supply the strongest academic defense of these three functions from different angles²⁸. Leeper (1991) and Woodford (1996) further show: even accepting these defenses, price stability still requires fiscal–monetary joint coordination across tools—a single anchor does not imply seigniorage must remain permanently monopolized²⁹; Calomiris’ s emphasis on

last-resort cost—moral hazard and political capture—reminds us monopoly defense and monopoly cost must appear on the same table³⁰. But monopoly cost is also real: artificially raised participation thresholds, politically blocked innovation paths, systemic squeeze of monetary power on vulnerable groups. The popularization pursuit is, while acknowledging monopoly value, systematically lowering its cost—not abolishing rational defense of monopoly.

Seigniorage has always coexisted with power, and power always reconfigures before technological change. We are in early stage of such reconfiguration—noisy, risky, and full of institutional possibilities rare before. Monopoly has reasons and costs; protocols lower participation thresholds, not responsibility; transition is long, direction is visible. Protocol is written, nodes run, rules are public. The rest of the story will be written jointly by code, markets, and rule of law—and we are all participants in this story, not spectators.

The value internet is not one company's product, not one government's decision, not one technologist's invention. It is institutional reality sedimented jointly by code countless engineers wrote, risk countless entrepreneurs bore, rules countless regulators examined and adjusted, and choices countless ordinary users expressed in action. This attribute of common creation is itself the truest interpretation of "popularization"—writing has begun; everyone who participates holds the pen.

注释与引用

1. BIS (2023), *The Future Monetary System* (Annual Economic Report, Chapter III), § III.B–III.C: tokenized deposits, wholesale CBDCs, and unified ledger as three main lines; BIS Innovation Hub, "Project mBridge" (2024 MVP), "Project Dunbar" (2022 PoC): multilateral CBDC cross-border settlement coexisting with SWIFT. <https://www.bis.org/publ/arpdf/ar2023e3.htm> ↩
2. BIS Committee on Payments and Market Infrastructures (2020), "Enhancing cross-border payments: building blocks of a global roadmap," Stage 1 report, § II–III (cross-border payment bottlenecks: compliance, FX, interoperability); IMF (2023), "Nigeria: Selected Issues," IMF Country Report 23/108, § 3 (eNaira low adoption and mobile-payment competition). <https://www.bis.org/cpmi/publ/d193.htm> ; <https://www.imf.org/en/Publications/CR/Issues/2023/02/07/Nigeria-Selected-Issues-529456> ↩
3. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008, §1–6 (double spending, timestamp chain, PoW consensus). <https://bitcoin.org/bitcoin.pdf> ↩
4. Szabo, Nick. "Money, Blockchains, and Social Scalability." *Unenumerated* blog, Feb. 2017 (verifiable rules lower interpersonal trust cost, social scalability). <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↩
5. Menger, Carl. "On the Origin of Money." *Economic Journal* 2(3), 1892, pp. 239–255 (saleability ranking, monetary emergence); English trans. in *The Origins of Money* (Mises Institute). <https://mises.org/library/origin-money-0> ↩
6. Schumpeter, Joseph A. *History of Economic Analysis*. Oxford University Press, 1954, Part II, ch. 6–7 (bank credit, deposit money, institutional succession); *Capitalism, Socialism and Democracy* (1942) creative destruction concept parallels monetary layer evolution. ↩
7. Knapp (1905/1924), *The State Theory of Money*, ch. 1 (tax anchor); Bagehot (1873), *Lombard Street*, ch. 2, 7 (last resort). See Chapter 24, Section 2 footnotes. ↩
8. Clarida, Gali & Gertler (1999), "The Science of Monetary Policy," *JEL* 37(4), pp. 1661–1707. <https://doi.org/10.1257/jel.37.4.1661> ↩
9. Bernanke et al. (1999), *Inflation Targeting*, ch. 1–2 (institutionalization of 2% anchor). Princeton 1999 ed. ↩ ↗²
10. Brunnermeier & Niepelt (2020), "On the Equivalence of Private and Public Money," *JME* 106, pp. 27–41. <https://doi.org/10.1016/j.jmoneco.2019.10.006> ↩ ↗²

11. Kindleberger, Charles P. *Manias, Panics, and Crashes*. 4th ed., Wiley, 2000, ch. 14 (Eurodollar, offshore dollar clearing); Eichengreen, Barry. *Globalizing Capital*. 2nd ed., Princeton, 2008, ch. 4–5 (Bretton Woods and offshore market tension). ↵
12. Eichengreen, Barry. *Globalizing Capital: A History of the International Monetary System*. 2nd ed., Princeton University Press, 2008, ch. 2–3 (classical gold standard, capital flows, convertibility discipline). ↵
13. Triffin, Robert. *Gold and the Dollar Crisis*. Yale University Press, 1960, ch. 1–2 (reserve currency domestic contradiction, Triffin dilemma). ↵
14. Keynes, John Maynard. *A Tract on Monetary Reform*. Macmillan, 1923, ch. 3 (short-term employment temptation vs long-term currency value; “In the long run we are all dead” context). <https://oll.libertyfund.org/titles/keynes-a-tract-on-monetary-reform> ↵
15. Woodford (2003), *Interest and Prices*, ch. 6–7; Galí (2015), *Monetary Policy, Inflation, and the Business Cycle*, 2nd ed., ch. 8, 15. See Chapter 24, Section 2 footnotes ⁹¹⁰. ↵
16. Ball, Laurence, N. Gregory Mankiw, and David Romer. “The New Keynesian Economics and the Output-Inflation Trade-off.” *Brookings Papers on Economic Activity*, 1988(1), pp. 1–65 (founding of New Keynesian synthesis); Walsh, Carl E. *Monetary Theory and Policy*. 4th ed., MIT Press, 2017, ch. 8–11 (NK benchmark, Taylor rule, ELB textbook pages). <https://doi.org/10.2307/2534423> ; MIT Press 2017 ed. ↵
17. Friedman, Milton. *A Program for Monetary Stability*. Fordham University Press, 1960. Ch. 4–5, pp. 65–93 (k% rule: constrains existing central bank, does not open private competition; rule execution still depends on institutional discretion). <https://fraser.stlouisfed.org/title/program-monetary-stability-3969> ↵
18. Eggertsson, Gauti B., and Michael Woodford. “The Zero Bound on Interest Rates and Optimal Monetary Policy.” *Brookings Papers on Economic Activity*, 2003(1), pp. 139–211 (k%-style fixed rules fail under ELB; unconventional tools or higher average inflation required). <https://doi.org/10.1353/eca.2003.0010> ↵
19. Blanchard, Dell'Ariccia & Mauro (2010), IMF SDN/10/03, pp. 1–18: post-crisis reflection whether 2% remains optimal; welfare trade-off of higher inflation target under recurring ELB. <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Rethinking-Macroeconomic-Policy-22486> ↵
20. Schmitt-Grohé & Uribe (2014), “Liquidity Traps and Letter of Last Resort Policies,” *AER* 104(5), pp. 110–115: under ELB optimal policy requires multi-tool joint coordination; no single fixed rule (central bank or on-chain) can bear macro stability alone. <https://doi.org/10.1257/aer.104.5.110> ↵
21. Kydland & Prescott (1977), “Rules Rather than Discretion,” *JPE* 85(3), pp. 473–491 (dynamic inconsistency; time inconsistency of discretionary constitution). <https://doi.org/10.1086/260580> ↵
22. Mises, Ludwig von. *Human Action*. Yale University Press, 1949, ch. 1, 4 (praxeology, subjective value, market process). <http://mises.org/library/human-action-0> ↵
23. Mr. Hayek (Hayek), 1976, *The Denationalization of Money*, ch. 24 “The Long-Run Prospects,” pp. 126–127: after competition weeds out failed experiments, several extensively used and very similar currencies will coexist; geographic boundaries blurred, border zones overlapping; not single currency winning all. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↵
24. Schumpeter, Joseph A. *History of Economic Analysis*. Oxford, 1954, Part II, ch. 6 (bank notes, paper credibility, central-bank rise); Fetter, Frank W. *Development of British Monetary Orthodoxy*. Harvard, 1965, ch. 7–9 (1844 Peel Act and issuance constraints). See Chapter 8, Section 1. ↵
25. Hayek, F. A. “The Results of Human Action but Not of Human Design.” In *Studies in Philosophy, Politics and Economics*, Routledge, 1967; also *Individualism and Economic Order* (1948) ch. 1, 6 (spontaneous order, dispersed knowledge). <https://oll.libertyfund.org/titles/hayek-individualism-and-economic-order> ↵
26. Marx, Karl. *Capital*, Vol. I, ch. 1–3 (commodity, value form, money as general equivalent); Chinese trans. *Capital* Vol. I Part I. <https://oll.libertyfund.org/titles/marx-capital-vol-i> ↵
27. Mr. Hayek (Hayek), 1976, *The Denationalization of Money*, ch. 1, 23: competition must weaken legal monopoly and forced legal tender; discipline from market choice not benevolence; PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↵
28. Synthesizes three strongest defense lines—state money theory (Knapp–Innes–Wray), New Keynesian inflation targeting (Woodford–Galí–Clarida), MMT fiscal space (Wray–Kelton)—with functional-division response. ↵

29. Leeper, Eric M. "Equilibria under 'active' and 'passive' monetary and fiscal policies." *Journal of Monetary Economics* 27(1), 1991, pp. 129–147 (fiscal/monetary active–passive combinations; single anchor does not imply seigniorage monopoly). [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q) ↩
30. Calomiris (1989), "Deposit Insurance: Lessons from the Record," *Economic Perspectives*, Chicago Fed, pp. 2–41 (last-resort cost side). <https://www.chicagofed.org/publications/economic-perspectives/1989/05> ↩

§ 27 Bad Money Exits: Popular Minting and Free Choice

Chapter in brief: Can ISO 4217 fiat symbols have a one-to-one, auditable public-domain representation on-chain? PCIM answers: yes, with supply constrained by collateral and referenda. Minting is not central-bank rationing but an economic choice after staking collateral; fiat whose monetary policy fails—and its on-chain mapping—may be marginalized in parallel comparison by not being chosen. This is a long-run vision, to be tested with corridor data. Openverse / VRC-10 is one implementation instance of PCIM.

Earlier chapters covered protocol verifiability and PCIM mechanics; this chapter condenses the Bitcurrency institutional picture into a core claim: global fiat mapped on public protocols; minting rights understood as holders' economic choice; how failed monetary policy and its on-chain mapping lose function in parallel competition by not being chosen—here "bad money drives out bad money" takes its literal competitive sense, not Gresham's law under fixed parities. What follows is a long-run institutional vision, to be tested by adoption, compliance interfaces, and corridor data.

Section 1 Protocol Mapping of Global Fiat

This section focuses on institutional meaning: rewriting the global fiat symbol table into composable public assets so cross-border and machine-readable scenarios need not rely on a single private stablecoin issuer's balance-sheet promise.

The modern international economy uses ISO 4217 as a symbol-layer convention: USD, EUR, CNY, JPY, and two hundred-plus fiat units share accounting language in cross-border messages, trade invoices, and central bank balance sheets. Symbols do not create purchasing power, but let sovereign units of account speak in one language—Goodhart summarizes this as the long coexistence of M-money (unit of account / legal-tender circle) and C-money (medium of exchange / store of value)¹. PCIM protocolizes that symbol layer: on the public chain, each standard fiat unit maps to a Bitcurrency-named asset (e.g. Bitcurrency-USD, Bitcurrency-EUR), issued under volatile-collateral over-collateralization and on-chain verifiable mint/redeem rules—not as liability certificates from a single private issuer.

Implementation example (Openverse): On Openverse's public chain, the interface standard is VRC-10; collateral is Bitgold; mint/redeem rules live in the protocol state machine; third parties can independently read the Bright-PCIM peg bound (tier mechanism in Chapter 14, Section 2.2).

The core proposition is **mapping, not replacement**: Bitcurrency names align with ISO 4217 units and aim to reproduce approximately stable purchasing power of that unit in open ecosystems, but does not claim overnight abolition of legal tender and tax anchors in each sovereign domestic sphere. Knapp's *State Theory of Money* ties money to the state through the tax-recycling circle—the state accepts domestic currency for taxes, conferring legal tender and unit-of-account status²; Innes and later Chartalist tradition summarize the same logic as "money from debt and settlement"³. In domestic retail, wages, and public spending, this circle will long lock local currency—the protocol path offers verifiable parallel discipline in off-anchor scenarios, not full replacement of the M-money layer. This section therefore asks: when value must settle cross-domain on-chain, be machine-readably referenced, and face third-party audit, can there exist a public representation aligned with sovereign symbols yet with supply constrained by open rules? The white paper's roadmap for two hundred-plus fiat public currencies is an engineering response; its real boundary is breadth of mapping depending on legal recognition, redemption channels, and OTC depth—not deployment code alone.

Distinguish layers from centralized stablecoins: USDT, USDC, etc. are liabilities on issuer balance sheets; reserve transparency depends on institutional audit and regulatory enforcement. Public Bitcurrency (VRC-10 on Openverse) writes currently effective tier collateral ratios, mint/redeem parity, and reserve R into the protocol state machine (tier mechanism in Chapter 14, Section 2.2); third parties can independently read peg-deviation upper bounds. Mapping does not preset which fiat's on-chain representation "wins"—only that competition can unfold under one interface standard, consistent with Hayek's vision of parallel currencies in *The Denationalization of Money*: "Good money cannot come from the benevolent intentions of a monopolist of money supply"⁴; competitive units shift from nineteenth-century banknotes to collateral issuance quotas under a unified public interface (VRC-10 on Openverse). Global main circulation medium means only public-layer Bitcurrency; VRC-11 Privcurrency serves licensed trade circles and does not enter this chapter's public comparison of "bad money exit."

Adoption gradients must be faced honestly: developed-economy retail and tax payment still lock local currency; on-chain mapping first accumulates liquidity in cross-border B2B, open-ecosystem internal pricing, and high-inflation marginal store-of-value. Ma et al. (2023) show stablecoin flows in stress periods highly synchronized with crypto market liquidity⁵; marginal-corridor adoption reflects exit options when fiat anchors fail—TVL cannot extrapolate global retail switch. Protocol mapping is therefore an infrastructure hypothesis, not a factual claim that "retail has already switched rails" (payment-volume metrics in Chapter 1, Section 8).

Scalability and verifiability of mapping must sit together: the protocol layer can add new fiat symbols, but each mapping needs independent OTC depth, compliance licenses, and merchant acceptance; symbol-table expansion does not equal equal expansion of C-money function. Complete mapping gives later competition "completeness of comparable objects"—only when all sovereign units can in principle be represented can bad-money exit appear as competition among mappings in the public layer, not a binary of "whether there is an on-chain exit."

Section 2 Minting as Choice

If the previous section answers "what on-chain symbols denote each fiat unit," this section answers "who expands on-chain supply of that unit under what discipline." PCIM transforms part of issuance from central-bank monopoly balance sheet into a protocol action any participant meeting collateral conditions may trigger: hold Bitgold, stake at the currently effective tier, mint corresponding Bitcurrency (circulation-tier referenda required to raise tier—Chapter 14, Section 2.2); redemption contracts supply and unlocks collateral. Minting is not administrative rationing but economic choice—locking volatile BTG as collateral for a stable unit in exchange for public-currency positions for circulation, settlement, and composition in the ecosystem.

"Popular" must be precise: technically any address meeting collateral and compliance may participate; in practice breadth depends on Bitgold distribution, operational thresholds, and legal attitude. Competitive issuance is therefore participation structure, not census "everyone mints": minting rights partly shift from unauditable meeting rooms to readable smart contracts and multi-issuer competition; discipline partly shifts from institutional reputation to collateral ratios, redemption arbitrage, and governance timelocks. Mises in *The Theory of Money and Credit* stressed that credit expansion without real savings correspondence eventually erodes purchasing power⁶; Friedman in *A Program for Monetary Stability* advocated $k\%$ rules constraining existing central banks, not opening private competition—rules still executed by committees, not independently verifiable by third parties⁷. PCIM's C_0 and on-chain C_0 share an "anti-discretion" lineage; the split is whether the executor can perform countercyclical functions at the ELB—PCIM does not replicate lender of last resort, but pushes marginal issuance verifiability forward. Selgin in *The Theory of Free Banking* further shows: when banknotes circulate at market

discount and overissued notes trade at discount, the public spends discounted notes first—competitive issuance discipline can be endogenous to clearing discounts, not administrative rationing⁸.

For regulators, minting as choice means observable issuance discipline: no need to wait for CPI to debate monetary over-issuance; on-chain collateral coverage and mint velocity offer higher-frequency reference for cross-border corridor supervision than quarterly institutional reports—reference does not replace macro-prudence, but narrows "talk stable, act loose" information asymmetry. For holders it means executable exit: redeem Bcurrency, unlock BTG, shift to other mappings or off-chain assets—institutionalized exit, speed constrained by ϵ and OTC depth, direction written in protocol, not issuer goodwill.

Minting as choice also means not minting is a choice: when a fiat unit's on-chain mapping persistently de-pegs, governance is captured, or compliance bans raise redemption cost, rational participants reduce new minting of that unit and shift to mappings with adequate collateral, deeper liquidity, clearer legal interfaces. Competitive issuance offers no moral guarantee that "good money necessarily drives out bad"—only institutional conditions that lower choice cost to protocol readability: holders need not wait for central bank minutes to observe on-chain collateral coverage, reserve drawdown, and mint velocity. Six operational points of competitive issuance gain behavioral meaning here: entry and exit at will, supply observability scaled to block time, make "choice" frequency far above traditional monetary policy committee cycles.

Mapping and minting must be read jointly: ISO 4217 provides the symbol map; PCIM provides supply games beneath symbols. Mint rhythm scaled to block time partly transforms "monetary policy" in the public layer into observable state variables—marginal changes central bank minutes take weeks to parse may be read in real time on block explorers: total collateral market cap, circulating Bcurrency supply, reserve R consumption, governance proposal queue. Transparency does not automatically improve distributive justice, but changes accountability structure: abuse must appear as visible collateral unlock or parameter-change proposals, not only lagged statistics of purchasing-power dilution.

Distinguish minting right from seigniorage: under PCIM, new minting must lock BTG; participants bear collateral price risk—unlike fiat fiscal monetization's implicit levy, unlike Anchor-style high-yield subsidies attracting deposits—the latter subsidize depositors with token inflation, inducing sophisticated-first exit when subsidies fade. Competitive issuance therefore refuses two temptations: neither "costless minting" nor "deposit equals yield" Ponzi gradients; minting is active choice bearing collateral risk.

Open questions remain: when multiple mappings run in parallel, whether arbitrage bandwidth ϵ and cross-venue depth (Barbon & Rinaldo 2024)⁹ suffice to maintain peg comparability across mappings; whether Bitgold concentration makes "popular" degenerate into whale issuance—still to be tested in practice.

Section 3 What "Bad Money Drives Out Bad Money" Means in Parallel Competition

Minting addresses who expands supply; parallel competition addresses how failed supply loses position in the market. Before mechanisms, nail terminology again: this chapter's "bad money" is not Gresham's legally overvalued coin, not Chapter 5's shield that "competition always means bad money wins"; but sovereign fiat whose monetary policy persistently fails, purchasing-power credibility erodes, on-chain mapping cannot maintain verifiable discipline, and its public representation. Exit is functional elimination: the unit may survive in domestic tax documents and ISO tables, but is no longer default-chosen in global C-money for cross-border settlement, open-ecosystem pricing, and long-term store of value.

This chapter's title takes "bad money drives out bad money" in literal competitive sense, must be distinguished from Gresham's law (institutional premises in Chapter 5)¹⁰. "Bad money" here means failed

monetary policy, on-chain mapping unable to maintain verifiable discipline; exit is functional elimination—symbols may remain in ISO and tax documents, but no longer default-chosen in global C-money.

Here bad money is: sovereign fiat with persistently failed monetary policy, eroded purchasing-power credibility, issuance discipline not third-party verifiable, and its Bitcurrency representation on-chain if mapped yet unable to maintain adequate collateral and credible redemption. Exit means functional disappearance, not physical destruction: symbols may remain in ISO and tax documents, but in cross-border settlement, open-ecosystem pricing, and long-term store of value, holders, merchants, and protocol routers no longer voluntarily choose it; liquidity and acceptance shrink to domestic M-money or marginal arbitrage gaps. This is not prophecy of a country's "collapse," but competitive logic: when multiple mappings run in parallel and switching cost falls via VRC standards, units with worse discipline and lower transparency lose C-money function first.

"Bad money drives out bad money" is therefore screening among peers: when on-chain dollar mapping coexists with on-chain high-inflation local mapping, if the latter lacks redemption depth, governance frequently lowers C_0 , or reserve disclosure triggers run coordination (Ahmed et al. 2024), the worse loses public circulation first—not simply dollar mapping "defeating" high-inflation currency, but when failed monetary policy gains on-chain representation, it must compete on stage with other mappings under equally open audit, and the failed exits first. Terra/UST teaches algorithmic under-collateralization's death spiral in confidence crises; PCIM belongs to over-collateralized CDP lineage, but cannot infer mapping auto-superiority—governance capture, thin-market pegs, and cross-protocol BTG contention can still make worse mappings lose function before better ones.

Linking Chapter 5: test whether parities can float, whether quality signals are cheaply verifiable. Standard interfaces lower switching cost; holders of failed mappings can redeem BTG and remind toward better-collateralized mappings—raising elimination speed ceiling without guaranteeing fairness (retail may still lag in bubbles).

The rift between domestic legal-tender circle and public C-money can long coexist: tax payment still requires local currency nominally, cross-border defaults to Bitcurrency—Goodhart's dual concepts appear as spatial division, not instant unification. Bad-money exit is directional—possibility (parallel mappings comparable) does not equal actuality (elimination complete). In transition, domestic retail may remain local-currency dominant; exit first occurs in off-anchor C-money; long-run, if mapping persistently fails, its on-chain representation marginalizes like local currency—not gaining "on-chain shelter."

Section 4 Who Stays and Who Is Marginalized

Empirical edge of parallel competition must condense to debatable screening criteria, not naming countries. This book does not hard-code which countries "win" or "exit"—institutional evolution depends jointly on political line, international goodwill, and compliance mutual recognition; any single-year map may be rewritten by war, sanctions, or regulatory sandboxes. What can be stated are structural conditions: which mappings more likely retain public circulation-medium status, which more likely retreat to domestic tax circles or licensed private domains.

Conditions more likely to retain mainstream mapping include: (1) monetary policy credibility and verifiable discipline—sovereign inflation targets or fiscal rules relatively stable, on-chain mapping maintains C_0 , reserve R , auditable redemption channels; (2) liquidity and interoperability depth—cross-chain routing, OTC, and exchange listings keep arbitrage bandwidth ϵ manageable, mapping becomes default quote unit in DeFi and payment stacks; (3) compliance interfaces and international goodwill—regulatory sandboxes, cross-border CBDC bridge trials (BIS mBridge, Dunbar), bilateral payment cooperation lower institutional adoption friction; politically willing to include on-chain mapping in auditable open financial infrastructure, not only as capital-control substitute; (4)

diplomatic and reserve politics acceptability—cross-border clearing media bear balance-sheet risk of foreign central banks and firms; mapping issuer countries must maintain international trust on sanctions, AML, and reserve transparency. (3)(4) show mainstream mapping is not purely technical—international goodwill and institutional openness are implicit collateral of C-money adoption.

Mappings more likely marginalized include: units with long-run monetary policy failure and on-chain mapping unable to maintain credible redemption; protocols with frequent governance capture, unilateral expansion in crises; legal environments fully banning public redemption channels, forcing mapping to degenerate into non-interconvertible IOUs; mappings with only narrative premium, lacking real payment scenes and OTC depth. Friedman and Schwartz in *A Monetary History of the United States* trace: monetary policy failure is not abstract but recognizable institutional trajectory—over-issuance, deposit-insurance moral hazard, and confidence collapse often follow in sequence¹¹. Marginalization does not equal domestic fiat disappearance—tax anchor and legal tender can sustain M-money—but public global circulation concentrates toward few mappings with better discipline and thicker liquidity.

Who stays and who marginalizes is therefore a marginal long-run equilibrium hypothesis: in parallel period all ISO units can in principle be mapped, but C-money function converges toward few mappings; when Bitcurrency is fully used domestically, it parallels sovereign currency—wages may still be paid in local currency, cross-border and on-chain default to Bitcurrency units, coexisting via instant exchange and dual accounting. Political choice to close programmable CBDC and suppress public redemption may delay but not necessarily eliminate marginal-corridor mapping demand—history shows capital and rules find gaps.

Corporate treasury and agent economies will accelerate screening: multinational on-chain treasury, machine-readable quotes, and autonomous agent micropayments (Part VI chapters) naturally favor mappings with deep liquidity, unified interface standards, stable oracle definitions—not cultural preference but hard constraints of automated settlement. Routing protocols cannot maintain equal default paths for two hundred thin mappings; convergence pressure therefore partly from tech stack, partly from political trust. Sanctions, AML cooperation, and bilateral swap arrangements can materially expand or compress specific mapping OTC corridors—international goodwill is not moral rhetoric but implicit collateral of C-money adoption.

Section 5 The Return of Monetary Power

The preceding propositions converge on the book's core political-economy claim: monetary power returns to participants and verifiable rules, not to anarchy or a new single oligopoly. Global symbol mapping, minting as choice, bad-money exit in parallel competition, and reserve-circulation division together close the Bitcurrency institutional picture. This section gathers five threads directly tied to the book's theme.

Popularization: issuance and audit participation open from licensed oligopoly to broad subjects meeting collateral and compliance; informationally, on-chain collateral ratios, mint velocity, and governance proposals are readable—but "can participate" does not automatically mean "everyone understands"; financial literacy and interface tools remain bottlenecks.

Elastic supply: PCIM adjusts supply with collateral within protocol bounds, unlike Bitcoin's fixed cap; elasticity does not equal fiscal-monetary countercyclical coordination, only marginal adjustment under verifiable rules, not meeting-room discretion.

Decentralization: no single issuer, multi-client and cross-jurisdiction nodes lower risk that shutting one point kills rules; decentralization does not eliminate governance capture and oracle concentration—must combine with timelocks and split-track quorums.

Power return: holders vote by minting, holding, redeeming; merchants and protocols vote by acceptance and liquidity; regulators vote by compliance interfaces and sandbox boundaries—power diffuses from "unchallengeable monopoly minting" to open multi-party games; domestic tax anchor and lender of last resort remain sovereign, not erased by this book.

Free choice: under parallel mappings, individuals and firms choose units with better discipline in off-anchor scenarios; legal tender constraints in domestic retail can coexist with public choice—Hayekian competitive discipline works at the margin without waiting for overnight abolition of legal tender¹². Choice includes not holding: when all visible mappings lack discipline, participants may return to off-chain assets, gold, or centralized stablecoins—parallel elimination is therefore relative, not absolute winner-take-all. Keynes in *General Theory* Chapter 13 characterized liquidity preference as opportunity cost of holding money¹³—in the mapping era, this extends to multidimensional calculation of "which verifiable unit to hold."

These themes with "bad money drives out bad money" and reserve-circulation division close the Bitcurrency institutional loop. Hayek in *Denationalization* Chapter 24 foresaw that after competitive elimination of failed experiments, the free world would host several extensively used, similar currencies—geographic dominant-currency boundaries blurred. In the protocol era, eliminated units shift from bank personas to mapping liquidity and verifiable discipline; blurred boundaries appear as routing default depth and OTC corridors, not map lines vanishing.

Monopoly minting's legitimacy comes from unified accounting, crisis liquidity, and financial stability; its cost is participation barriers and implicit levy. Popularization seeks to systematically lower the latter while acknowledging the former—not declaring state exit from money, but declaring: on the public on-chain domain, the failed must face auditable alternative mappings; the sound must continuously prove discipline through redemption and collateral. Rules are written in protocol; details of elimination and convergence still need time and practice.

注释与引用

1. Goodhart, Charles A. E. "The two concepts of money." *European Journal of Political Economy* 14(3), 1998, pp. 407–432. ↩
2. Knapp, Georg Friedrich. *The State Theory of Money*. Macmillan, 1924, ch. 1. <https://oll.libertyfund.org/titles/knapp-the-state-theory-of-money> ↩
3. Innes, A. Mitchell. "What is Money?" *Banking Law Journal*, May 1913; Wray, L. Randall. *Modern Money Theory* (2012). ↩
4. Hayek (1976), *The Denationalization of Money*, p. 23. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
5. Ma, Ganesh, Andreas Schimpf, and Andreas V. I. Pereira. "Stablecoins amid Crypto Winter." IMF WP 23/72, 2023. ↩
6. Mises, Ludwig von. *The Theory of Money and Credit*. Yale, 1953, Part III, ch. 17–20. <https://mises.org/library/theory-money-and-credit> ↩
7. Friedman, Milton. *A Program for Monetary Stability*. Fordham, 1960, ch. 4–5. <https://fraser.stlouisfed.org/title/program-monetary-stability-3969> ↩
8. Selgin, George. *The Theory of Free Banking*. Rowman & Littlefield, 1988, ch. 3. ↩
9. Barbon, Andrea, and Angelo Rinaldo. arXiv:2112.07386. ↩
10. Hayek (1976), pp. 42–43 on Gresham under fixed legal rates. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩
11. Friedman & Schwartz. *A Monetary History of the United States*. Princeton, 1963, ch. 4, 7. ↩
12. Hayek (1976), ch. 22 "The Problem of Transition." ↩

13. Keynes, J. M. *The General Theory*. Macmillan, 1936, ch. 13. <https://oll.libertyfund.org/titles/keynes-the-general-theory> ↗

§ 28 The Endgame of Money

Earlier chapters covered mapping, minting, bad-money exit, and power return; this chapter turns to functional division of reserve and circulation: in the long-run equilibrium of the public value internet, Bitgold (BTG) with fixed supply bears world reserve function; global circulation medium converges toward few (this book does not preset specific countries) VRC-10 Bitcurrency mappings, not two hundred-plus equal mappings. Reserve-layer and circulation-layer division answers an old question in Hayek and Goodhart traditions: can store-of-value anchor and daily circulation medium separate, and how should they? What follows remains long-run vision; convergence speed and mapping count depend on liquidity, compliance, and geopolitics.

Section 1 Two-Layer Monetary Structure

Traditional fiat systems already have internal hierarchy: M0, M1, M2 separate circulation and deposit money; internationally, foreign reserves and settlement currencies divide roles—the dollar often plays both, inviting Triffin-style tension from one currency bearing too many functions¹. PCIM and the white paper's functional constraints on Bitgold offer an explicit protocol-layered extreme statement: BTG total supply about 200 million, halving roughly every three years, main monetary-economic use as collateral base for public and private currency issuance; everyday Bitcurrency retail payment is borne by VRC-10, BTG itself not as mass circulation medium.

Reserve layer (Bitgold) functionally approaches gold's record and constraint layer under the gold standard: supply discipline anchored by protocol cap and halving rhythm, price market-discovered, providing hard collateral and POS security stake for upper-layer constant-value units. Fisher in *Stabilizing the Dollar* envisioned index rules partly stripping "value measure" from political discretion²; Szabo's bit gold turned verifiable scarcity and proof-of-work precursors into on-chain reserve hypothesis³. Circulation layer (VRC-10 Bitcurrency) maps ISO 4217 units, maintains approximately constant purchasing power via dynamic-tier over-collateralization and mint/redeem arbitrage (upper tier $C_0 \approx 161.8\%$), bearing cross-border settlement, open-ecosystem pricing, and machine-readable value-layer medium functions. Two layers rigidly link through PCIM mint/redeem: circulation expansion must lock reserve-layer positions, contraction releases BTG—accounting mirror similar to some central banks' "FX holdings—domestic money creation," but collateral state on-chain readable, redemption rules not dependent on single-institution promise.

Emphasis: reserve—circulation layering applies only to public VRC-10; VRC-11 Privcurrency at 61.8% low collateral serves licensed trade circles, not global main circulation competition. Global main circulation medium means only public Bitcurrency; Privcurrency is private settlement tool, not comparison object for bad-money exit narrative.

Section 2 Why Reserve Should Be "One," Circulation Can Be "Few"

Reserve layer tends toward "one," circulation layer permits "few," from different dimensions of scale economy and trust cost.

Reserve should be "one": fragmented global store-of-value anchors raise cross-mapping arbitrage, collateral contention, and clearing counterparty risk together. The white paper says Bitgold has "only one monetary-economic use"—as collateral base for issuance—aiming to avoid native token simultaneously as payment medium, speculation target, and governance chip. Single standard asset with fixed supply lets all VRC-10 mappings share one hard-collateral market depth and price discovery; if each mapping bound different reserve assets, three-layer BTG contention (VRC-10/11/12 simultaneous expansion) would tighten coverage. One here is protocol

simplification and unified collateral hypothesis, not assertion humans abandon gold, Treasuries, and other off-chain reserves—on-chain world reserve and off-chain central bank reserves long coexist.

Circulation should be "few": two hundred-plus ISO mappings deployable technically, but C-money network effects, OTC depth, and merchant default pricing units bias toward few head media. White in *Future of Money in the Information Age* asks whether unit of account can converge when multiple private monies coexist⁴; Hayek in *Denationalization* long-run prospects foresees several extensively used, similar currencies after competitive elimination, geographic boundaries blurred⁵. Menger long noted competitive issuance's hardest closure is not note authenticity but whose price list is standard⁶. In the public layer, "few" means cross-border and open-ecosystem default acceptance converges toward one or two mappings with thickest liquidity, clearest compliance interfaces, highest monetary policy credibility—this book does not fix which sovereign they must correspond to, only states structural tendency of convergence.

Most mappings may still exist serving bilateral trade, regional ecosystems, dedicated corridors, but global main circulation medium function does not distribute equally across two hundred units.

Two-layer combination clarifies division logic: dynamic circulation borne by few Bitcurrency; static discipline constrained by fixed-supply BTG; elastic supply occurs at circulation layer (collateral increase/decrease), reserve layer supply curve lacks central-bank-style discretionary expansion—unless governance rewrites cap, at very high political and market cost. Mises in *Human Action* links monetary supply elasticity to subjective actors' expectation coordination⁷—in protocol era, elasticity bounds written in C_0 and redemption rules, not central bank minutes.

Section 3 Parallel Relation with Domestic Currency

Bitcurrency is sovereign domestic currency's extended on-chain representation, not simple invasion of alien "foreign money." Vision of full adoption: domestic economy may still parallel local currency—wages, tax, public contracts may remain fiat-denominated; cross-border, on-chain settlement, open ecosystems, and machine-agent payment default to Bitcurrency mapping units; the two link via instant exchange, dual-track accounting, and CBDC/bank interfaces. Brunnermeier and Niepelt equivalence reminds: parallel units must convert to public anchor, fiscal must recycle liquidity spillover; else degenerate into non-interconvertible IOU markets.

Parallel does not mean 1:1 legal parity: on-chain mapping maintains purchasing power via collateral and redemption, domestic currency via tax anchor and central bank balance sheet—marginal parities should approach but allow deviation within arbitrage bandwidth ϵ . High-inflation domestic currency may retain legal tender domestically while on-chain mapping with better discipline sees C-money circle shift first; rift between domestic M-money and global C-money has precedent in Zimbabwe dollarization. Keynes in *Tract on Monetary Reform* opposed treating short-run exchange manipulation as long-run prosperity tool⁸—mapping parallel must prevent misreading on-chain convenience as infinite deviation from sovereign parity magic. Full use means enterprises and individuals do not "abandon local currency" but layer by scenario: domestic retail local currency, international settlement Bitcurrency—like today enterprises hold local working capital, dollar cross-border invoices.

Transition reality: fiat-dominant retail will continue years. Parallel starts cross-border, supply chain, marginal corridors, penetrates domestic dual-track; generational scale, if mapping continuously proves discipline and convenience, acceptance may expand, but tax anchor does not auto-vanish—popularization is marginal extension, not overnight domestic single-rail replacement.

Section 4 Convergence Picture

Projecting institutional logic to long cycle yields a cautious convergence picture (not a forecast timetable):

Phase A (present–next decade): fiat and CBDC dominate domestic retail; USDT/USDC and few public mappings contest liquidity in cross-border and DeFi; two hundred-plus Bitcurrency mappings deployable technically, most depth thin in practice.

Phase B (transition accumulation): compliance interfaces and interoperability standards (VTP, MiCA-class frameworks) give some mappings institutional redemption channels; marginal substitution expands in cross-border B2B, compute markets, agent micropayments; mappings of monetary-policy-failed entities lose public position first under parallel competition logic.

Phase C (long-run equilibrium hypothesis): global C-money circulation converges toward few VRC-10 Bitcurrency + single BTG reserve layer—few means functional main media count, not political monetary union declaration; BTG as on-chain world reserve collateral, head mappings as dynamic circulation and pricing; domestic M-money still mainly each country's currency, paralleling mappings.

Convergence does not mean ISO table shrinks or sovereignty vanishes; means public global circulation network effects concentrate toward few units, failed mappings marginalized. Schumpeter's "creative destruction" in *Capitalism, Socialism and Democracy* reminds: old layers do not exit quietly but are marginalized when new tools prove comparative advantage⁹. Hayekian blurred geographic boundaries in protocol era appear as: same merchant may quote multiple mappings, but liquidity routing defaults to deepest—market sorting replaces legal-parity sorting.

Section 5 Closing the Book on the Popularization of Money

The book titled *The Popularization of Money*, subtitle *A New Chapter in Monetary Civilization: Tribal Tokens • State Fiat • Popular Protocol • Value in Direct Flow*, closes civilizational scale in four arcs; intellectually it follows and goes beyond Hayek's *Denationalization*: what changes is discipline carrier and participation structure, not abolishing exchange and settlement. The last two chapters of Part VII close against the book's theme in seven mutually supporting propositions:

Popularization: minting and audit participation open from oligopoly to broad subjects under verifiable rules; responsibility and risk diffuse together, not promise of universal enrichment.

Elastic supply: circulation layer adjusts with collateral; unlike Bitcoin rigid cap, unlike opaque central bank discretion—elasticity bounds written in C_0 , R , governance timelocks.

Decentralization: issuance without single institution, rules run multi-copy; not no governance, not no compliance interface.

Power return: holding, minting, redemption, acceptance circles constitute exit voting; sovereign tax anchor and lender of last resort remain, but monopoly minting must face auditable alternatives.

Free choice: off-anchor scenarios choose mappings with better discipline; domestic legal tender can long coexist with public choice.

Bad money drives out bad money: failed monetary policy and its on-chain mapping lose C-money function in parallel competition by not being chosen—not Gresham legal parity.

Bitgold world reserve: fixed-supply BTG as unified reserve-layer collateral; few Bitcurrency as global circulation layer—reserve "one," medium "few" functional layering.

Seven in one: money in the value-internet era need not be less, but must be more verifiable; need not be stateless, but must have less unchallengeable monopoly discretion. State, central bank, law do not vanish; what vanishes is the single-path fantasy that "only the monopolist may issue and cannot be audited."

Section 6 Unfinished Business

Crisis liquidity: protocols lack Bagehot-style lender of last resort; in systemic deleveraging, on-chain redemption and fiat liquidity may dry up together¹⁰. PCIM cannot replace central bank crisis function, only offers exit options for pricing and store of value.

Mainnet and evidence: Bright-PCIM peg bound, mechanism stability, bad-money exit, and convergence picture all need stress data, governance events, and cross-border adoption panels—white paper roadmap cannot substitute empirics.

Governance and capture: parameter transparency does not equal anti-capture; concentrated holdings, crisis expansion proposals may still erode C_0 .

Regulation and asymmetry: unilateral bans, reserve reviews, payment licenses can quickly reshape mapping landscape; international goodwill and political line are implicit adoption variables technology cannot unilaterally decide.

Cognition and fairness: on-chain readable does not mean everyone can read; popularization benefiting only professional analysts is new elitism.

Quantum and cryptography migration: long-run infrastructure upgrade cost and execution cycle cannot be underestimated.

Unit-of-account convergence: ERC-20/VRC lower switching cost, do not auto-solve "whose price list is standard"—White's problem persists in mapping era.

Unfinished business is not declaration of failure but research agenda: monetary popularization is ongoing institutional experiment, not perfect tense. Rules are written in protocol, nodes are running; subsequent story is co-written by code, markets, rule of law, and every participant's choice—with cautious hope worth holding while acknowledging boundaries.

Section 7 A Further Thought: Does Money Die?

Money will not be abolished; the state monopoly of the mint prerogative will—this section's title probes whether the category of money generalizes, not abolishing exchange media (central thesis in preface and Chapter 24).

The convergence picture above still takes VRC-10 Bitcurrency as public main circulation medium and Bitgold as unified reserve—fiat retreats in C-money circle, parallels few mappings. Push the horizon one step further and a question this book has less developed appears.

When fiat continuously retreats in cross-border settlement, open ecosystems, and machine-readable value layer, circulation may not long converge to binary "few nominal fiat mappings + single reserve." Openverse white paper's VRC suite beyond VRC-10 public currency includes VRC-11 private stablecoin, VRC-12 security tokens, VRC-13 time tokens—VRC-10/11/12 take Bitgold as collateral core; VRC-13 backed by service commitments, settlement may still route via BTG reserve layer but is not BTG-collateral issuance family. They serve different scenes: licensed trade settlement, asset equity transfer, professional service commitments. If collateral discipline is verifiable and standard interfaces interoperable, assets issued on the BTG reserve chain and service-

commitment tokens may bear pricing, payment, and clearing in respective acceptance circles—sharing reserve anchor or off-chain performance constraints, yet no longer neatly folding into single "Bitcurrency" medium image.

In this vista, what "money" denotes may shift. Classically money must alternately or jointly serve exchange medium, unit of account, store of value; when the value internet turns every collateralizable, redeemable, composable on-chain position into potential payment means, circulation medium seems to diffuse from monopoly of few sovereign symbols to parallel multi-layer assets atop reserve system—exchange and clearing still occur, unit of account may still converge on few deep head mappings, but boundary of "which token counts as money" blurs: today we ask "pay dollars or bitcoin," tomorrow perhaps "pay Bitcurrency, Privcurrency, some RWA share, or instantly splittable portfolio?"

Does this mean death of money?

Money will not be abolished; the state monopoly of the mint prerogative will¹¹. On that reading, the vista more likely describes generalization of monetary form, not disappearance of monetary function—Mengerian saleability and Szaboian social scalability¹² still need some commonly accepted clearing layer and pricing anchor; Bitgold reserve layer provides verifiable hard constraint so "everything payable" does not slide to "nothing comparable."

But the question cannot close. If fiat retreats on a long enough scale from C-money while BTG-based assets broadly replace "single money" intuition in respective scenes, do textbook M0/M1/M2 layering, central bank balance-sheet centrality, and "money" as independent policy variable still hold? Marx in *Capital* Vol. I Part II–III dialectically links money and capital forms—expansion of monetary function does not auto-cancel social determination of value measure¹³. Or we witness post-monetary state: what does not vanish is value transfer and bookkeeping; what vanishes is single-rail imagination binding circulation medium to sovereign persona—"money" degenerates to generic term for "BTG-collateral-chain-constrained circulating claims," policy discussion shifts from "how much domestic currency to issue" to "reserve coverage and cross-asset clearing rules."

This book cannot settle this question. It may be popularization's logical endpoint—reserve one, media plural, money as category dissolving into verifiable asset spectrum; or over-extrapolation—humans may still cry for few simple pricing units in chaos, like QWERTY persisting before better layouts. Worth keeping is the question itself: when fiat retreats and BTG-reserve-issued assets all circulate, do we arrive at popularization of money or end of money as concept? Answer will not come from white paper but from holders, merchants, regulators, and autonomous systems' actual choices in every payment route over coming decades.

Rules are written in protocol; whether "money" remains a necessary word still awaits history's writing.

注释与引用

1. Triffin, Robert. *Gold and the Dollar Crisis*. Yale, 1960; Eichengreen, Barry. *Globalizing Capital*. Princeton, 2008. ↩
2. Fisher, Irving. *Stabilizing the Dollar*. Macmillan, 1920, ch. 1–3. ↩
3. Szabo, Nick. "Bit gold." *Unenumerated*, Dec. 2005; Openverse *Bitgold Whitepaper* v2.1.5. <https://unenumerated.blogspot.com/2005/12/bit-gold.html> ↩
4. White, Lawrence H. "Competing Money, Free Banking, and the Unit of Account." *Cato*, 1994. ↩
5. Hayek, F. A. *The Denationalization of Money*. IEA, 1976, ch. 24. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↩

6. Menger, Carl. "On the Origin of Money." *Economic Journal* 2(3), 1892. <https://mises.org/library/origin-money-0> ↵
7. Mises, Ludwig von. *Human Action*. Yale, 1949, ch. 17. <https://mises.org/library/human-action-0> ↵
8. Keynes, J. M. *A Tract on Monetary Reform*. Macmillan, 1923. <https://oll.libertyfund.org/titles/keynes-a-tract-on-monetary-reform> ↵
9. Schumpeter, Joseph A. *Capitalism, Socialism and Democracy*. Harper, 1942, ch. 7. ↵
10. Bagehot, Walter. *Lombard Street*. 1873, ch. 2, 7. ↵
11. Hayek (1976), ch. 1. PDF: <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf> ↵
12. Menger (1892); Szabo (2017) "Money, Blockchains, and Social Scalability." <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html> ↵
13. Marx, Karl. *Capital*, Vol. I, Part II–III, ch. 4–6. <https://oll.libertyfund.org/titles/marx-capital-vol-i> ↵

Bibliography

Bibliography

A–H

- Fisher, Irving. *The Purchasing Power of Money: Its Determination and Relation to Credit, Interest, and Crises*. Macmillan, 1911 (rev. ed.). English translation: <https://fraser.stlouisfed.org/title/purchasing-power-money-5379>
- Fisher, Irving. *Stabilizing the Dollar: A Plan to Stabilize the General Price Level Without Fixing Individual Prices*. Macmillan, 1920. PDF: https://fraser.stlouisfed.org/files/docs/publications/books/stabilizing_fisher.pdf
- Friedman, Milton. *Capitalism and Freedom*. University of Chicago Press, 1962.
- Friedman, Milton. "The Role of Monetary Policy." *American Economic Review* 58(1), March 1968, pp. 1–17. PDF: https://www.cooperative-individualism.org/friedman-milton_the-role-of-monetary-policy-1968-mar.pdf
- Friedman, Milton. *Counter-Revolution in Monetary Theory*. Wincott Memorial Lecture, Institute of Economic Affairs, Occasional Paper 33, 1970.
- Friedman, Milton, and Anna J. Schwartz. *A Monetary History of the United States, 1867–1960*. Princeton University Press, 1963.
- Hayek, F.A. *The Denationalization of Money*. Hobart Paper Special 70, Institute of Economic Affairs, 1976. <https://cdn.nakamotoinstitute.org/docs/Denationalization.pdf>
- Hayek, F.A. *Individualism and Economic Order*. University of Chicago Press, 1948.
- Hayek, F.A. *The Road to Serfdom*. University of Chicago Press, 1944.

K–M

- Keynes, John Maynard. *The General Theory of Employment, Interest and Money*. Macmillan, 1936. Marxists.org English translation: <https://www.marxists.org/reference/subject/economics/keynes/general-theory/>
- Keynes, John Maynard. *A Tract on Monetary Reform*. Macmillan, 1923. Project Gutenberg: <https://www.gutenberg.org/ebooks/32637>
- Menger, Carl. "On the Origin of Money." *Economic Journal*, 1892. English translation: https://cdn.mises.org/On%20the%20Origins%20of%20Money_5.pdf
- Marx, Karl. *Capital*, Vol. I. 1867. Marxists English translation: <https://www.marxists.org/archive/marx/works/1867-c1/>
- Chs. 1–3 (commodities, forms of money, circulation): <https://www.marxists.org/archive/marx/works/1867-c1/ch01.htm>
- Ch. 4 (general formula of capital $M—C—M'$): <https://www.marxists.org/archive/marx/works/1867-c1/ch04.htm>
- Marx, Karl. *A Contribution to the Critique of Political Economy*. 1859. Marxists English translation: <https://www.marxists.org/archive/marx/works/1859/critique-pol-economy/>
- Mises, Ludwig von. *The Theory of Money and Credit*. 1912. Liberty Fund English translation: <https://www.econlib.org/library/Mises/msT.html>
- Mises, Ludwig von. *Human Action: A Treatise on Economics*. Yale University Press, 1949. English translation: <https://www.econlib.org/library/Mises/HmA/msHmA.html>

- Say, Jean-Baptiste. *Traité d'économie politique*. 1803. Vol. 1, Ch. 15 ("products are bought with products" / Say's Law): English excerpt <https://la.utexas.edu/users/hcleaver/368/368SayTreatiseBk1Ch15table.pdf>

N–R

- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." October 2008. <https://bitcoin.org/bitcoin.pdf>
- Rockoff, Hugh. "The Free Banking Era: A Reexamination." *Journal of Money, Credit and Banking* 6(2), May 1974, pp. 141–167. <https://doi.org/10.2307/1990856>
- Rolnick, Arthur J., and Warren E. Weber. "Gresham's Law or Gresham's Fallacy?" *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1986, pp. 17–30. <https://www.minneapolisfed.org/research/quarterly-review/greshams-law-or-greshams-fallacy>
- Bresciani-Turroni, Costantino. *The Economics of Inflation: A Study of Currency Depreciation in Post-War Germany*. 1931. English ed., 1937. Ch. 4 (Weimar; Hayek *Denationalization* p. 43 cites p. 174 on distrust vs fixed rates). <https://www.econlib.org/library/Bresciani-Turroni/btEI.html>
- Jevons, W. Stanley. *Money and the Mechanism of Exchange*. Appleton, 1875. Ch. 8 (Spencer free coinage; Hayek cites pp. 64–65, 82). <https://www.gutenberg.org/ebooks/12792>
- Hanke, Steve H., and Nicholas Krus. "World Hyperinflations." Cato Working Paper, 2013. Zimbabwe Hyperinflation Index updated through November 2008. <https://www.cato.org/research/working-papers/world-hyperinflations>
- Rockoff, Hugh. "Lessons from the American Experience with Free Banking." In Kevin Dowd (ed.), *The Experience of Free Banking*. Routledge, 1992, ch. 4, pp. 73–86.
- Dowd, Kevin (ed.). *The Experience of Free Banking*. Routledge, 1992.
- Calomiris, Charles W. "Deposit Insurance: Lessons from the Record." *Economic Perspectives*, Federal Reserve Bank of Chicago, May/June 1989, pp. 2–41. <https://www.chicagofed.org/publications/economic-perspectives/1989/05>
- Kroszner, Randall S. "Free Banking: The Scottish Experience as a Model for Emerging Economies?" *Review*, Federal Reserve Bank of St. Louis, March/April 1996, pp. 25–31. https://files.stlouisfed.org/files/htdocs/publications/review/96/03/FreeBanking_Mar_Apr1996.pdf
- Selgin, George. *The Theory of Free Banking: Money Supply under Competitive Note Issue*. Rowman & Littlefield, 1988. <https://www.econlib.org/library/Selgin/selTheory.html>
- Selgin, George. "Synthetic Commodity Money." *Journal of Financial Stability* 17, 2015, pp. 92–99. <https://doi.org/10.1016/j.jfs.2015.01.002>
- Selgin, George, and Lawrence H. White. "How Would the Invisible Hand Handle Money?" *Journal of Economic Literature* 32(4), December 1994, pp. 1718–1749. <https://doi.org/10.1257/jel.32.4.1718>
- White, Lawrence H. *Free Banking in Britain: Theory, Experience, and Debate, 1800–1845*. Cambridge University Press, 1995 (2nd ed.); 1st ed. 1984, Ch. 2, pp. 40–52 (option clause); Ch. 4, pp. 76–95 (clearing networks).
- White, Lawrence H. "The Scottish Banking System before 1845: A Model for Laissez-Faire?" *Journal of Money, Credit and Banking* 27(2), May 1995, pp. 421–431. <https://doi.org/10.2307/2077878>

- White, Lawrence H. "Competitive Payments Systems and the Unit of Account." *American Economic Review* 84(3), June 1994, pp. 699–712.
- White, Lawrence H. *Competition and Currency: Essays on Free Banking and Money*. New York University Press, 1989. Ch. 1–3 (free-banking theory survey); Ch. 4 (Scottish option clause and clearing networks).
- Selgin, George. "The Case for Free Banking: Then and Now." *Cato Journal* 10(3), Winter 1991, pp. 539–552. <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1990/11/cj10n3-1.pdf>
- Selgin, George. "The Suppression of State Banknotes: A Reconsideration." *Economic Inquiry* 48(4), October 2010, pp. 931–942 (institutional consequences of the 1865 federal tax suppressing state banknotes and "par laws"). <https://doi.org/10.1111/j.1465-7295.2009.00260.x>
- Selgin, George. "Bank Deregulation and Monetary Order." In *The Cato Handbook for Congress*, Cato Institute, 1995, pp. 249–262 (modern policy implications of competitive issue and clearinghouse discipline).
- Rolnick, Arthur J., and Warren E. Weber. "New Evidence on the Free Banking Era." *American Economic Review* 78(5), December 1988, pp. 880–890 (bond-collateral rules and interstate failure-rate differences). <https://doi.org/10.1257/aer.78.5.880>
- Rolnick, Arthur J., and Warren E. Weber. "Explaining the Demand for Free Bank Notes." *Journal of Monetary Economics* 21(1), January 1988, pp. 47–71. [https://doi.org/10.1016/0304-3932\(88\)90004-5](https://doi.org/10.1016/0304-3932(88)90004-5)
- Weber, Warren E. "Resolving the Free Banking Debate." *Federal Reserve Bank of Minneapolis Quarterly Review*, September 1994, pp. 2–8 (Scottish vs U.S. experience contrasted; weight of institutional detail). <https://www.minneapolisfed.org/research/quarterly-review/resolving-the-free-banking-debate>
- Spencer, Richard W. "The Number of Banks in the United States, 1790–1860." *Journal of Economic History* 25(3), September 1965, pp. 421–428. <https://doi.org/10.1017/S0022050700056217>
- Dowd, Kevin. *Laissez-Faire Banking*. Routledge, 1993. Ch. 2–4 (competitive-issue models and clearinghouse-endogenized discipline).
- White, Lawrence H. *Free Banking in Britain: Theory, Experience, and Debate, 1800–1845*. Cambridge University Press, 1984 (1st ed.). Ch. 2, pp. 40–52 (option clause: deferred redemption + compensatory interest); Ch. 4, pp. 76–95 (spontaneous clearing networks). 2nd ed. 1995: see N–R section above. Cambridge 1984 edition.
- Selgin, George. "The Evolution of a Free Banking System." *Economic Inquiry* 22(3), July 1984, pp. 289–300 (evolutionary path of competitive issue—discount clearing—clearinghouse discipline; precursor to Selgin 1988 monograph). <https://doi.org/10.1111/j.1465-7295.1984.tb01270.x>
- Dwyer, Gerald P. "Wildcat Banking in the United States." *Federal Reserve Bank of Richmond Economic Review*, 79(1), January/February 1993, pp. 1–20 (wildcat banking geographic arbitrage; *Bank Note Reporter* authentication costs). https://www.richmondfed.org/publications/research/economic_review/1993/er7901
- Dwyer, Gerald P. "Wildcat Banking, Banking Panics, and Free Banking in the United States." *Economic Inquiry* 34(4), October 1996, pp. 881–889 (wildcat banking coexisting with free-banking laws; authentication costs determine retention of inferior notes). <https://doi.org/10.1111/j.1465-7295.1996.tb00123.x>
- Timberlake, Richard H. "The Central Banking Role of Clearinghouse Associations." *Journal of Money, Credit and Banking* 16(1), February 1984, pp. 1–15 (clearinghouse suspension of convertibility, peer monitoring; complementary to Dowd 1993 model). <https://doi.org/10.2307/1992521>

- Selgin, George. "The Legal Restrictions Theory of Money: A Reappraisal." *Cato Journal* 6(1), Spring/Summer 1986, pp. 479–497 (legal restrictions vs free banking; institutional prehistory of the 1865 suppression of state banknotes). <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/1986/5/cj6n1-4.pdf>

Free-Banking School and Historiographical Debates (Further Reading)

Directly relevant to the free-banking—Thiers—Gresham dialogue in Chapters 4, 5, and 7; prefer citing these over secondary surveys.

- Calomiris, Charles W., and Stephen H. Haber. *Fragile by Design: The Political Origins of Banking Crises and Scarce Credit*. Princeton University Press, 2014. Ch. 2 (Scotland vs U.S. institutional political economy; counter to the White/Selgin narrative).
- Kroszner, Randall S. "The Economics of Central Bank Independence." In *Central Bank Independence, Targets, and Credibility*, Cato Institute, 1996, pp. 1–12 (policy context of the free-banking debate and central-bank independence).
- White, Lawrence H. "Free Banking in Scotland before 1844." In Kevin Dowd (ed.), *The Experience of Free Banking*, Routledge, 1992, ch. 5, pp. 87–102.
- Rockoff, Hugh. "The Wizard of Oz as a Monetary Allegory." *Journal of Political Economy* 98(4), August 1990, pp. 739–760 (historiographical background to the 1896 par-law debate; intersects Selgin 2010 on state-banknote suppression).

S–Z

- Schumpeter, Joseph. *Capitalism, Socialism and Democracy*. Harper & Brothers, 1942.
- Schumpeter, Joseph. *History of Economic Analysis*. Oxford University Press, 1954.
- Szabo, Nick. "Bit gold." *Unenumerated*, December 2005. <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
- Bank for International Settlements. *Central Bank Digital Currencies: Foundational Principles and Core Features*. Joint report, October 2020. <https://www.bis.org/publ/othp33.htm>
- Bank for International Settlements. *The Future Monetary System*. Annual Economic Report, Chapter III, June 2023. <https://www.bis.org/publ/arpdf/ar2023e3.htm>
- MakerDAO. *The Dai Stablecoin System: White Paper* (v0.1). December 2017. Source: official white paper v0.1; not independently audited. <https://makerdao.com/en/whitepaper/>
- Ricks, Morgan, John Crawford, and Lev Menand. "FedAccounts: Digital Dollars." *George Washington Law Review* 89(1), 2020. <https://www.gwlr.org/fedaccounts-digital-dollars/>
- Financial Stability Board. *Assessment of Risks to Financial Stability from Crypto-assets*. October 2022. <https://www.fsb.org/2022/10/assessment-of-risks-to-financial-stability-from-crypto-assets/>
- Openverse Foundation. *Bitgold Whitepaper* v2.1.5. Source: official white paper v2.1.5; not independently audited. https://cdn.openverse.network/english/Openverse%20Whitepaper/Bitgold_whitepaper_en_2.1.5.pdf
- Openverse Foundation. *VRC-11 Privcurrency Bluepaper* v2.0.0. Source: official blue paper v2.0.0; not independently audited. https://cdn.openverse.network/docs/openverse_vrc11_privcurrency_bluepaper_2.0.0.pdf

Modern Monetary Economics, Stablecoins, and DeFi Empirics

- Kiyotaki, Nobuhiro, and Randall Wright. "On Money as a Medium of Exchange." *Journal of Political Economy* 97(4), August 1989, pp. 927–954. <https://doi.org/10.1086/261634>
- Kiyotaki, Nobuhiro, and Randall Wright. "A Search-Theoretic Approach to Monetary Economics." *American Economic Review* 83(1), March 1993, pp. 63–77. <https://doi.org/10.1257/aer.83.1.63>
- Knapp, Georg Friedrich. *The State Theory of Money (Staatliche Theorie des Geldes)*. 1905. English ed., Macmillan, 1924. Ch. 1 (chartalism, unit of account). <https://archive.org/details/statetheoryofmon030559mbp>
- Goodhart, Charles A. E. "The two concepts of money: implications for the analysis of optimal currency areas." *Economic Journal* 108(447), 1998, pp. 377–390. Reprinted in *European Journal of Economics and Economic Policies: Intervention* 1(1), 2004, pp. 9–23 (chartalism vs metallism; tax anchor vs collateral anchor). <https://doi.org/10.1111/1468-0297.00291>
- Innes, A. Mitchell. "What is Money?" *Banking Law Journal*, May 1913, 30(5); "The Credit Theory of Money." *Banking Law Journal*, Dec. 1914, 31(12). Reprint: <https://www.community-exchange.org/docs/Innes/>
- Bagehot, Walter. *Lombard Street: A Description of the Money Market*. Henry S. King, 1873. Ch. 2, 7 (lender of last resort). <https://www.gutenberg.org/ebooks/4359>
- Wray, L. Randall. *Modern Money Theory: A Primer on Macroeconomics for Sovereign Monetary Systems*. Palgrave Macmillan, 2012. Ch. 2 (taxes create currency demand), Ch. 5–6 (fiscal space).
- Woodford, Michael. *Interest and Prices: Foundations of a Theory of Monetary Policy*. Princeton University Press, 2003. Ch. 6 (optimal inflation under nominal rigidities, pp. 235–280); Ch. 7 (zero lower bound and ELB policy, pp. 281–330).
- Galí, Jordi. *Monetary Policy, Inflation, and the Business Cycle*. Princeton University Press, 2nd ed., 2015. Ch. 8 (New Keynesian optimal monetary policy, pp. 145–180); Ch. 15 (flexible inflation targeting and discretion–commitment trade-offs, pp. 320–340).
- Kelton, Stephanie. *The Deficit Myth*. PublicAffairs, 2020.
- Galí, Jordi, and Tommaso Monacelli. "Optimal Monetary and Fiscal Policy in a Currency Union." *Journal of International Economics* 76(1), 2008, pp. 116–132. <https://doi.org/10.1016/j.jinteco.2008.08.003>
- Sargent, Thomas J., and Neil Wallace. "Some Unpleasant Monetarist Arithmetic." *Federal Reserve Bank of Minneapolis Quarterly Review*, Fall 1981, pp. 1–17: under high deficits, if the central bank accommodates fiscal financing at low rates, higher inflation must eventually validate the debt. <https://www.minneapolisfed.org/research/quarterly-review/some-unpleasant-monetarist-arithmetic>
- Taylor, John B. "Discretion versus Policy Rules in Practice." *Carnegie-Rochester Conference Series on Public Policy* 39, 1993, pp. 195–214 (Taylor rule: inflation gap + output gap; empirical benchmark for FIT). [https://doi.org/10.1016/0167-2231\(93\)90009-L](https://doi.org/10.1016/0167-2231(93)90009-L)
- Taylor, John B. "A Historical Analysis of Monetary Policy Rules." In *Monetary Policy Rules*, University of Chicago Press, 1999, ch. 1, pp. 9–54 (1790s–1990s historical comparison of rules vs discretion). <https://doi.org/10.7208/chicago/9780226791258.001.0001>
- Leeper, Eric M. "Equilibria under 'active' and 'passive' monetary and fiscal policies." *Journal of Monetary Economics* 27(1), 1991, pp. 129–147 (active/passive monetary–fiscal pairs and price-level equilibria). [https://doi.org/10.1016/0304-3932\(91\)90007-Q](https://doi.org/10.1016/0304-3932(91)90007-Q)

- Woodford, Michael. "Control of the Public Debt: A Requirement for Price Stability?" In *NBER Macroeconomics Annual 1996*, vol. 11, MIT Press, 1996, pp. 143–169 (public-debt dynamics and price stability; dialogue with Sargent–Wallace 1981). <https://doi.org/10.1086/654291>
- Sargent, Thomas J. "The Ends of Four Big Inflations." In *Inflation: Causes and Effects*, University of Chicago Press, 1982, pp. 41–98 (ends of four big inflations: fiscal reform + rebuilding the monetary anchor). <https://doi.org/10.7208/chicago/9780226312705.001.0001>
- Rotemberg, Julio J., and Michael Woodford. "An Optimization-Based Econometric Framework for the Evaluation of Monetary Policy." In *NBER Macroeconomics Annual 1997*, vol. 12, MIT Press, 1997, pp. 297–346 (New Keynesian DSGE policy-evaluation framework). <https://doi.org/10.1086/654340>
- Christiano, Lawrence J., Martin Eichenbaum, and Charles L. Evans. "Nominal Rigidities and the Dynamic Effects of a Shock to Monetary Policy." *Journal of Political Economy* 113(1), February 2005, pp. 1–45 (Calvo pricing + habit formation; dynamics of monetary-policy shocks). <https://doi.org/10.1086/426038>
- Smets, Frank, and Rafael Wouters. "Shocks and Frictions in US Business Cycles: A Bayesian DSGE Approach." *American Economic Review* 97(3), June 2007, pp. 586–606 (euro-area/Fed DSGE benchmark models; empirical FIT calibration). <https://doi.org/10.1257/aer.97.3.586>
- McCallum, Bennett T. "Issues in the Design of Monetary Policy Rules." In *Handbook of Macroeconomics*, vol. 1, Elsevier, 1999, ch. 23, pp. 1483–1530 (rule design: targets vs instruments, time-varying natural rate). [https://doi.org/10.1016/S1574-0048\(99\)10034-7](https://doi.org/10.1016/S1574-0048(99)10034-7)
- Sargent, Thomas J., and Neil Wallace. "Rational Expectations and the Theory of Economic Policy." *Journal of Political Economy* 84(2), April 1976, pp. 241–254 (policy rules and rational expectations; precursor to the 1981 arithmetic). <https://doi.org/10.1086/260448>
- Kydland, Finn E., and Edward C. Prescott. "Rules Rather than Discretion: The Inconsistency of Optimal Plans." *Journal of Political Economy* 85(3), June 1977, pp. 473–491. <https://doi.org/10.1086/260580>
- Clarida, Richard, Jordi Galí, and Mark Gertler. "The Science of Monetary Policy: A New Keynesian Perspective." *Journal of Economic Literature* 37(4), December 1999, pp. 1661–1707. <https://doi.org/10.1257/jel.37.4.1661>
- Eggertsson, Gauti B., and Michael Woodford. "The Zero Bound on Interest Rates and Optimal Monetary Policy." *Brookings Papers on Economic Activity*, 2003(1), pp. 139–211. <https://doi.org/10.1353/eca.2003.0010>
- Ball, Laurence, N. Gregory Mankiw, and David Romer. "The New Keynesian Economics and the Output-Inflation Trade-off." *Brookings Papers on Economic Activity*, 1988(1), pp. 1–65 (foundational New Keynesian synthesis survey; nominal rigidities + expectation anchoring). <https://doi.org/10.2307/2534423>
- Walsh, Carl E. *Monetary Theory and Policy*. 4th ed., MIT Press, 2017. Ch. 8–11 (New Keynesian baseline model, Taylor rule, optimal monetary policy, and ELB; textbook-grade checkable pages). MIT Press 2017 edition.
- Orphanides, Athanasios. "The Quest for Prosperity Without Inflation." *Journal of Monetary Economics* 50(3), April 2003, pp. 715–730 (1960s–1990s historical Taylor-rule deviations and inflation consequences; contrast with forward-guidance misjudgment). [https://doi.org/10.1016/S0304-3932\(03\)00028-7](https://doi.org/10.1016/S0304-3932(03)00028-7)
- Canzoneri, Matthew B., Robert E. Cumby, and Behzad Diba. "Is the Price Level Determined by the Needs of Fiscal Solvency?" *American Economic Review* 91(5), December 2001, pp. 1221–1238 (fiscal solvency

constraint and price-level determination; dialogue with Leeper 1991 and Sargent–Wallace 1981).
<https://doi.org/10.1257/aer.91.5.1221>

- Bassetto, Marco, and Todd Messer. "Fiscal Consequences of the Federal Reserve's Actions During the Financial Crisis." Federal Reserve Bank of Chicago Working Paper 2013-13, 2013, pp. 1–35 (crisis unconventional operations and the fiscal–monetary boundary; contemporary extension of unpleasant arithmetic). <https://doi.org/10.21033/wp-2013-13>
- Sims, Christopher A. "A Simple Model for Study of the Determination of the Price Level and the Interaction of Monetary and Fiscal Policy." *Economic Theory* 4(3), 1994, pp. 381–399 (minimal FTPL model; read with Leeper active–passive mix). <https://doi.org/10.1007/BF01215355>
- Del Negro, Marco, Marc P. Giannoni, and Frank Schorfheide. "Inflation in the Great Recession and New Keynesian Models." *American Economic Journal: Macroeconomics* 7(1), January 2015, pp. 168–196 (DSGE benchmark forecasts of post-2008 inflation/deflation; estimable FIT empirics). <https://doi.org/10.1257/mac.2013.029>
- Woodford, Michael. "Convergence in Macroeconomics: Elements of the New Synthesis." *American Economic Journal: Macroeconomics* 1(1), January 2009, pp. 267–279. <https://doi.org/10.1257/mac.1.1.267>
- Sargent, Thomas J. *The Conquest of American Inflation*. Princeton University Press, 1999. Ch. 2–3 (rational expectations and inflation anchoring; Volcker disinflation).
- Sargent, Thomas J., and Neil Wallace. "Rational Expectations and the Dynamics of Hyperinflation." In *Rational Expectations and Economic Policy*, Federal Reserve Bank of Minneapolis, 1980, pp. 73–110.
- Bernanke, Ben S., Thomas Laubach, Frederic S. Mishkin, and Adam S. Posen. *Inflation Targeting: Lessons from the International Experience*. Princeton University Press, 1999. Ch. 1–2 (institutionalization of inflation targeting and expectation anchoring).
- Blanchard, Olivier. "The Future of Macroeconomics after the Crisis." *Oxford Review of Economic Policy* 34(1–2), 2018, pp. i43–i49 (New Keynesian synthesis and post-crisis reflection). <https://doi.org/10.1093/oxrep/grx036>
- Blanchard, Olivier, Giovanni Dell'Ariccia, and Paolo Mauro. "Rethinking Macroeconomic Policy." IMF Staff Discussion Note SDN/10/03, February 12, 2010, pp. 1–18 (post-crisis reflection: whether 2% remains optimal at the ELB; welfare trade-offs of a higher inflation target). <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Rethinking-Macroeconomic-Policy-22486>
- Bell, Stephanie A. "Can Taxes and Bonds Finance Government Spending?" *Journal of Economic Issues* 34(2), June 2000, pp. 603–620 (MMT operational layer: taxes drain reserves rather than "finance spending"). <https://doi.org/10.1080/00213624.2000.11506379>
- Fullwiler, Scott T. "Modern Money Theory and Interrelations between the Treasury and the Central Bank: An Operational and Institutional Analysis." Levy Economics Institute Working Paper No. 855, 2016, pp. 1–35 (MMT operational description: spending creates reserves, taxes destroy them, Treasuries adjust). <https://www.levyinstitute.org/publications/modern-money-theory-and-interrelations-between-the-treasury-and-the-central-bank>
- Goodhart, Charles A. E. *The Evolution of Central Banks: A Natural History*. MIT Press, 1988. Ch. 4–5 (lender of last resort as an ex-post institutionalized invention; moral hazard and deposit insurance). MIT Press 1988 edition.

- Mehrling, Perry. *The New Lombard Street: How the Fed Became the Dealer of Last Resort*. Princeton University Press, 2011. Ch. 1 (from Bagehot lender of last resort to the post-2008 "dealer of last resort"). Princeton 2011 edition.
- Schmitt-Grohé, Stephanie, and Martín Uribe. "Liquidity Traps and Letter of Last Resort Policies." *American Economic Review* 104(5), May 2014, pp. 110–115 (optimal ELB policy must tolerate inflation overshoot or fiscal coordination). <https://doi.org/10.1257/aer.104.5.110>
- Bindseil, Ulrich. *Central Bank Digital Currency: Considerations, Projects, Outlook*. ECB Occasional Paper Series 322, 2024. <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op322~5822218919.en.pdf>
- Bindseil, Ulrich, Fabio Panetta, and Ignacio Terol. "Central Bank Digital Currency: Functional Scope, Pricing and Controls." ECB Occasional Paper Series 286, December 2021. <https://ssrn.com/abstract=3975939>
- Bindseil, Ulrich. "Tiered CBDC and the Financial System." ECB Working Paper 2351, January 2020. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf>
- Holston, Kathryn, Thomas Laubach, and John C. Williams. "Measuring the Natural Rate of Interest: International Trends and Determinants." *International Journal of Central Banking* 13(5), 2017, pp. 55–76. <https://doi.org/10.20955/ijcb.2017.55.55>
- Bank for International Settlements. "Estimating the natural rate of interest in an open economy." BIS Working Paper 1067, August 2023. <https://www.bis.org/publ/work1067.htm>
- Carapella, William, and Leland D. Fleischman. "Wholesale central bank digital currency: payments innovation, and the case for implementation." *FEDS Notes*, Board of Governors of the Federal Reserve System, September 25, 2020. <https://www.federalreserve.gov/econres/notes/feds-notes/wholesale-central-bank-digital-currency-payments-innovation-and-the-case-for-implementation-20200925.html>
- Bank for International Settlements, Committee on Payments and Market Infrastructures. "Enhancing cross-border payments: building blocks of a global roadmap." Stage 1 report, July 2020. <https://www.bis.org/cpmi/publ/d193.htm>
- Bank for International Settlements, Committee on Payments and Market Infrastructures. "Central bank digital currencies: financial stability implications." *BIS Papers* No. 113, September 2021. <https://www.bis.org/publ/bppdf/bispap113.htm>
- International Monetary Fund. "Nigeria: Selected Issues." IMF Country Report 23/108, February 2023, §3 (eNaira adoption vs mobile money). <https://www.imf.org/en/Publications/CR/Issues/2023/02/07/Nigeria-Selected-Issues-529456>
- Niepelt, Dirk. *Central Bank Digital Currency: Whence, Why, What, and How*. MIT Press, 2024. Ch. 2–4 (taxonomy and architecture); Ch. 5–6 (retail CBDC and fiscal-central-bank division of labor). <https://mitpress.mit.edu/9780262047555/central-bank-digital-currency/>
- Niepelt, Dirk. "Money and Banking with Reserves and CBDC." *Journal of Finance* 79(4), August 2024, pp. 2505–2552. <https://www.niepelt.ch/files/jf2024.pre.pdf>
- Assenmacher, Katrin, and Frank Smets. "A digital euro: monetary policy considerations." SUERF Policy Note 346, 2024. <https://www.suerf.org/publications/suerf-policy-notes-and-briefs/a-digital-euro-monetary-policy-considerations/>

- Brunnermeier, Markus K., Harold James, and Jean-Pierre Landau. "The digitalization of money." NBER Working Paper 26300, September 2019. Also BIS Working Paper 941. <https://www.bis.org/publ/work941.pdf>
- Brunnermeier, Markus K., and Jean-Pierre Landau. "The digital euro: policy implications and perspectives." Study for the European Parliament ECON Committee, 2022. [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733783/IPOL_STU\(2022\)733783_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733783/IPOL_STU(2022)733783_EN.pdf)
- Brunnermeier, Markus K., and Dirk Niepelt. "On the Equivalence of Private and Public Money." *Journal of Monetary Economics* 106, 2020, pp. 27–41. <https://doi.org/10.1016/j.jmoneco.2019.10.006>
- Barrdear, John, and Michael Kumhof. "The macroeconomics of central bank issued digital currencies." *BIS Working Paper* 488, July 2016, pp. 5–12. <https://www.bis.org/publ/work488.htm>
- Chiu, Jonathan, Seyed Mohammad R. Davoodalhosseini, Janet Hua Jiang, and Yu Zhu. "Bank Market Power and Central Bank Digital Currency: Theory and Quantitative Assessment." *Journal of Political Economy* 131(5), May 2023, pp. 1213–1248 (orig. Bank of Canada Staff Working Paper 19-20, 2019). <https://doi.org/10.1086/722075>
- Andolfatto, David. "Assessing the Impact of Central Bank Digital Currency on Private Banks." *Federal Reserve Bank of St. Louis Review* 103(2), 2021, pp. 153–175. <https://www.stlouisfed.org/publications/review/2021/02/05/assessing-the-impact-of-central-bank-digital-currency-on-private-banks>
- Brunnermeier, Markus K., and Yann Koby. "The Reversal Interest Rate." *American Economic Review* 109(8), August 2019, pp. 2615–2647. <https://doi.org/10.1257/aer.20181007>
- Fernández-Villaverde, Jesús, and Daniel Sanches. "Can Currency Competition Work?" *Journal of Monetary Economics* 102, November 2019, pp. 1–15. <https://doi.org/10.1016/j.jmoneco.2018.08.004>
- Fernández-Villaverde, Jesús, Daniel Sanches, Linda Schilling, and Harald Uhlig. "Central bank digital currency: Central banking for all?" *Journal of Monetary Economics* 134, November 2023, pp. 1–15 (orig. NBER WP 26753, 2020). <https://doi.org/10.1016/j.jmoneco.2023.05.004>
- BIS Committee on Payments and Market Infrastructures. *Stablecoins: Implications for monetary policy, financial stability and the international monetary system*. Report, 2022. <https://www.bis.org/publ/othp31.htm>
- Auer, Raphael, Giulio Cornelli, and Jon Frost. "CBDC and financial stability." *BIS Quarterly Review*, March 2022, pp. 55–68. https://www.bis.org/publ/qtrpdf/r_qt2203e.htm
- BIS Innovation Hub. "Project mBridge: Connecting economies through CBDC." 2024 update (MVP phase). https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm
- Bank for International Settlements. "CBDCs: Progress and ongoing work." *BIS Papers* No. 125, July 2023 (86 central banks surveyed; 93% exploring CBDC). <https://www.bis.org/publ/bppdf/bispap125.htm>
- Boar, Corrado, Henry Holden, and Amber Wadsworth. "Ready, steady, go? Results of the third BIS survey on central bank digital currency." *BIS Papers* No. 114, January 2021. <https://www.bis.org/publ/bppdf/bispap114.htm>
- Boar, Corrado, Henry Holden, and Amber Wadsworth. "Impending arrival — a sequel to the survey on central bank digital currency." *BIS Quarterly Review*, March 2020, pp. 57–70. https://www.bis.org/publ/qtrpdf/r_qt2003e.htm

- Group of Central Banks and BIS. "Central bank digital currencies: system design and interoperability." Report, September 2021 (update to 2020 foundational principles). <https://www.bis.org/publ/othp38.htm>
- Agur, Itai, Anil Ari, and Giovanni Dell'Ariccia. "Designing central bank digital currencies." IMF Working Paper 19/252, September 2019. <https://www.imf.org/en/Publications/WP/Issues/2019/09/26/Designing-Central-Bank-Digital-Currencies-48655>
- Keister, Todd, and Cyril Monnet. "Central Bank Digital Currency: Stability and Information." Federal Reserve Bank of Philadelphia Working Paper 20-16, July 2020. <https://www.philadelphiafed.org/-/media/frbp/assets/working-papers/2020/wp20-16.pdf>
- Keister, Todd, and Cyril Monnet. "Central bank digital currency: Stability and information." *Journal of Economic Dynamics and Control* 142, 2022, article 104501 (OFR Working Paper 22-04). https://www.financialresearch.gov/working-papers/files/OFRwp-22-04_central-bank-digital-currency.pdf
- Meller, Barbara, and Oscar Soons. "Know your (holding) limits: CBDC, financial stability and central bank reliance." ECB Occasional Paper Series 326, 2024. <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op326~d5c223d9b4.en.pdf>
- Kumhof, Michael, and Clare Noone. "Central bank digital currencies — design principles for financial stability." BIS Working Paper 880, March 2021. <https://www.bis.org/publ/work880.htm>
- Mancini-Griffoli, Tommaso, et al. "Casting light on central bank digital currencies." IMF Staff Discussion Note 18/08, November 2018. <https://www.imf.org/en/Publications/WP/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-44542>
- Bank of England. *Central Bank Digital Currency: Opportunities, challenges and design*. Discussion Paper, March 2020. <https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper>
- European Central Bank. "Progress on the preparation phase of a digital euro." October 2023 (legislative package, holding limits, offline payments). https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
- People's Bank of China. *Progress of Research & Development of E-CNY in China*. White Paper, July 2021. Source: official white paper; not independently audited. <http://www.pbc.gov.cn/en/3688110/3688172/4157446/4296336/index.html>
- BIS Innovation Hub. "Project Dunbar: International settlements using multi-CBDC platforms." 2022 proof-of-concept (Australia, Malaysia, Singapore, South Africa). <https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm>
- BIS Innovation Hub, Saudi Central Bank, UAE CB. "Project Aber: Cross-border digital currency payments." 2020 proof-of-concept (dual-issued wholesale CBDC). <https://www.bis.org/about/bisih/topics/cbdc/aber.htm>
- Terra Form Labs. "Terra Money: Stability and Adoption." Whitepaper, April 2019. Source: official white paper v1; not independently audited. Internet Archive: https://web.archive.org/web/20210508125312/https://assets.website-files.com/611153587644a1b237457044/6112a3499a47a1d3d8d1b1c4_Terra_White_Paper.pdf
- Anchor Protocol. "Anchor Protocol White Paper." 2020. Source: official white paper; not independently audited; Terra/UST ecosystem high-yield deposit mechanism; terminated with the 2022 UST depeg. <https://anchorprotocol.com/docs/anchor-v1.pdf>

- International Monetary Fund. *Global Financial Stability Report*, October 2022, Chapter 2 ("The Crypto Ecosystem and Financial Stability Challenges"), pp. 43–78 (Terra/Luna collapse, stablecoin risks). <https://www.imf.org/en/Publications/GFSR/Issues/2022/10/11/global-financial-stability-report-october-2022>
- U.S. Securities and Exchange Commission. *Complaint: SEC v. Terraform Labs Pte. Ltd. et al.*, February 16, 2023 (UST/LUNA as unregistered securities; post-collapse legal anatomy). <https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-32.pdf>
- Brunnermeier, Markus K., Darius Niehaus, and Stefan Schab. "The DeFi Paradox." *BIS Bulletin* No. 63, 27 May 2022 (Terra/UST death spiral, DeFi–TradFi contagion channels). <https://www.bis.org/publ/bisbull63.htm>
- Liu, Jiageng, Igor Makarov, and Antoinette Schoar. "Anatomy of a Run: The Terra Luna Crash." NBER Working Paper 31160, April 2023 (blockchain run dynamics, Anchor subsidies, sophisticated-first exit). <https://www.nber.org/papers/w31160>
- Hong Kong Monetary Authority. "An Event Study on the May 2022 Stablecoin Market Crash." Research Memorandum RM09-2022 (algorithmic vs collateralized stablecoin run pressures). <https://www.hkma.gov.hk/media/eng/publication-and-research/research/research-memorandums/2022/RM09-2022.pdf>
- Board of Governors of the Federal Reserve System. "Interconnected DeFi: Ripple Effects from the Terra Collapse." FEDS Notes / Finance and Economics Discussion Series 2023-044 (cross-chain bridge spillover after Terra). <https://www.federalreserve.gov/econres/feds/files/2023044pap.pdf>
- Klages-Mundt, Fabian, et al. "Stablecoins 2.0: Economic foundations and risk-based models." *Journal of Financial Stability* 68, 2023, 101142. <https://doi.org/10.1016/j.jfs.2023.101142>
- Lyons, Richard K., and Ganesh Viswanath-Natraj. "What Keeps Stablecoins Stable?" NBER Working Paper 27136, May 2020 (revised 2022). <https://www.nber.org/papers/w27136>
- Viswanath-Natraj, Ganesh, and Richard K. Lyons. "Stable coins don't inflate? On the dynamics of USDC pricing." *Journal of International Money and Finance* 131, 2023, 102777. <https://doi.org/10.1016/j.jimonfin.2023.102777>
- Gorton, Gary, and Jeffery Zhang. "Taming Wildcat Stablecoins." *University of Chicago Law Review* 89(1), 2022, pp. 1–52. <https://lawreview.uchicago.edu/print-archive/taming-wildcat-stablecoins>
- Arner, Douglas W., Ross P. Buckley, and Moritz Schularick. "The Future of Stablecoins." *Journal of Financial Regulation* 8(2), 2022, pp. 155–179. <https://doi.org/10.1093/jfr/fjac010>
- Auer, Raphael, Giulio Cornelli, and Jon Frost. "DeFi lending: Intermediation without intermediators?" *BIS Quarterly Review*, December 2022, pp. 69–82 (MakerDAO/Compound lending anatomy). https://www.bis.org/publ/qtrpdf/r_qt2212f.htm
- Schär, Fabian. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." *Federal Reserve Bank of St. Louis Review* 103(2), 2021, pp. 153–174 (MakerDAO/DAI CDP overview). <https://www.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>
- MakerDAO. "The Maker Protocol: MakerDAO Purple Paper." 2019 (CDP, liquidation, DSR; Source: official technical white paper; not independently audited). <https://makerdao.com/en/whitepaper/makerdao-purple-paper/>

- MakerDAO Risk Team. "Black Thursday Post Mortem" (March 12, 2020): ETH -30%+ intraday, zero-bid auctions, DAI premium; subsequent governance raised ETH collateral ratios. Forum: <https://forum.makerdao.com/t/black-thursday-post-mortem/1853>
- Chitra, Tarun, et al. "Modeling and Analysis of Crypto-Backed Over-Collateralized Stable Derivatives in DeFi." *Frontiers in Blockchain* 7, 2024, 1392812 (DAISIM simulation, DAI peg belief parameter, ETH collateral risk). <https://doi.org/10.3389/fbloc.2024.1392812>
- S&P Global. "Stablecoins: A Deep Dive into Valuation and Depegging." Special Editorial, 2023 (DAI/USDC depeg event anatomy, peg deviation duration). <https://www.spglobal.com/content/dam/spglobal/corporate/en/images/general/special-editorial/stablecoinsadeepdiveintovaluationanddepegging.pdf>
- Chitra, Tarun, and Guillermo Angeris. "Improved Price Oracles: Constant Function Market Makers." *AFT* 2020. <https://arxiv.org/abs/2003.10001>
- Daian, Philip, et al. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." *IEEE S&P* 2020. <https://arxiv.org/abs/1904.05234>
- Qin, Kaihua, et al. "Quantifying Blockchain Extractable Value: How Dark is the Forest?" *IEEE S&P* 2022. <https://arxiv.org/abs/2101.05593>
- Angeris, Guillermo, et al. "An analysis of Uniswap markets." *Cryptoeconomic Systems* 2021. <https://arxiv.org/abs/1911.03380>
- Chainalysis. *The 2024 Geography of Cryptocurrency Report* (stablecoin adoption in high-inflation/emerging markets; regional payment intensity). <https://www.chainalysis.com/geography-of-crypto/>
- McKinsey & Company, Artemis Analytics. "Stablecoins in payments: What the raw transaction numbers miss." McKinsey Payments, 2025 (adjusted vs nominal on-chain volume; ~\$390B annual payment use). <https://www.mckinsey.com/industries/financial-services/our-insights/stablecoins-in-payments-what-the-raw-transaction-numbers-miss>
- Coin Metrics. *State of Stablecoins 2024* (market cap, peg deviation, reserve composition benchmarks). <https://coinmetrics.io/state-of-stablecoins/>
- Eisenberg, Sebastian, and Andreas Schär. "Decentralised Finance (DeFi): A functional approach." *ECB Macropprudential Bulletin*, Issue 25, November 2023, pp. 43–48 (MakerDAO, stablecoin lending, systemic links). https://www.ecb.europa.eu/pub/pdf/other/ecb.mpbu202305_25~fbfdbb0c39.en.pdf
- Artemis Analytics. "Stablecoin Metrics Dashboard & Methodology." 2024–2025 (nominal on-chain volume; cited in McKinsey adjusted payment estimates). <https://www.artemis.xyz/>
- BIS Committee on Payments and Market Infrastructures. "Application of the Principles for financial market infrastructures to stablecoin arrangements." Consultative report, July 2022. <https://www.bis.org/cpmi/publ/d198.htm>
- Commodity Futures Trading Commission. "CFTC Staff Report on DeFi and the Terra/Luna Collapse." Staff Report, 2022 (algorithmic stablecoin failure anatomy; death spiral mechanism). https://www.cftc.gov/media/8406/CFTCStaffReport_DeFiTerraLuna050222/download
- Gudgeon, Lewis, et al. "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency." *AFT* 2020. <https://arxiv.org/abs/2006.13221>

- Eisenberg, Sebastian, and Andreas Schär. "DeFi Liquidations: Mechanics, Returns, and Risks." *AFT* 2021. <https://arxiv.org/abs/2106.06398>
- Werner, Daniel, and Antonis Papadatos. "SoK: Decentralized Finance (DeFi) Attacks." *IEEE Access* 11, 2023, pp. 113847–113867 (oracle manipulation, governance attacks, liquidation cascades). <https://doi.org/10.1109/ACCESS.2023.3322018>
- Inter-American Development Bank. "Survey on the Use of Bitcoin in El Salvador." January 2022 (Chivo wallet adoption: ~12% regular users, ~70% cash-primary; counter-evidence to legal-tender-as-adoption narrative). <https://www.iadb.org/en/news/survey-use-bitcoin-el-salvador>
- Ortiz, Alvaro, and David Witte. "Stablecoin runs and the centralization of monetary systems." BIS Working Paper 1137, December 2023 (algorithmic vs collateralized stablecoin run dynamics; Terra/Luna post-mortem). <https://www.bis.org/publ/work1137.htm>
- Momtazi, Saeed. "Lessons Learned from the Terra-Luna Crash." *Journal of Risk and Financial Management* 15(11), 2022, 520. <https://doi.org/10.3390/jrfm15110520>
- Capponi, Agostino, Ruizhe Jia, and Ye Wang. "The Evolution of Market Structure in DeFi." *Management Science* (forthcoming), 2024 preprint (DEX liquidity, MEV, professional searchers vs retail). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4273980
- Cong, Lin William, Ye Li, and Neng Wang. "Tokenomics: Dynamic Adoption and Valuation." *Journal of Financial Economics* 151, 2024, pp. 103745 (DeFi incentive design, adoption dynamics; Anchor-style subsidy sustainability). <https://doi.org/10.1016/j.jfineco.2023.103745>
- Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf. "DeFi risks and the decentralisation illusion." *BIS Quarterly Review*, December 2021, pp. 21–36 (oracle, governance, and liquidity concentration; counter to permissionless narrative). https://www.bis.org/publ/qtrpdf/r_qt2112e.htm
- Lehar, Alfred, and Christine A. Parlour. "Decentralized Exchange: The Uniswap Automated Market Maker." *Journal of Finance* 80(1), February 2025, pp. 321–374 (DEX liquidity pools, AMM vs limit order book, MEV/arbitrage dynamics). <https://doi.org/10.1111/jofi.13405> ; SSRN: <https://ssrn.com/abstract=3905316>
- Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. "An empirical study of DeFi liquidations." *Proceedings of the 21st ACM Internet Measurement Conference (IMC)*, 2021, pp. 336–350 (MakerDAO/Aave/Compound/dYdX longitudinal liquidation data; Black Thursday auction mechanics). <https://doi.org/10.1145/3487552.3487811> ; arXiv: <https://arxiv.org/abs/2106.06389>
- Aspris, Angelo. "From Collateral to Liquidation: The impact of DeFi Leverage on Performance." SSRN Working Paper 4913633, February 2024 (Maker protocol vault-level leverage, stability fees, forced liquidations 2019–2023). <https://ssrn.com/abstract=4913633>
- Ma, Ye, Yan Ji, and Andreas Schrimpf. "Stablecoin Flows and Crypto Markets." IMF Working Paper 23/72, April 2023 (stablecoin flows during market stress; cross-border corridor adoption). <https://www.imf.org/en/Publications/WP/Issues/2023/04/21/Stablecoin-Flows-and-Crypto-Markets-532788>
- Barbon, Andrea, and Angelo Rinaldo. "On the Quality of Cryptocurrency Markets: Centralized versus Decentralized Exchanges." *Management Science* (forthcoming), 2024 preprint; DOI 10.1287/mnsc.2024.07703 (CEX vs DEX liquidity quality, gas fees and arbitrage deviations; complements Ferraro et al. 2022 thin-market peg analysis). arXiv: <https://arxiv.org/abs/2112.07386>

- Clements, Ryan. "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins." *Wake Forest Law Review Online* 11, October 2021, pp. 131–171 (algorithmic stablecoin three fragility conditions; Terra pre-mortem). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3952045
- Adams, Austin, and Markus Ibert. "Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel." *FEDS Notes*, Board of Governors of the Federal Reserve System, June 2, 2022. <https://doi.org/10.17016/2380-7172.3121>
- Ahmed, Rashad, Iñaki Aldasoro, and Chanelle Duley. "Public information and stablecoin runs." BIS Working Paper 1164, January 2024 (revised January 2025) (reserve quality disclosure paradox; global games run coordination). <https://www.bis.org/publ/work1164.htm>
- Auer, Raphael, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese, and Friedhelm Victor. "The Technology of Decentralized Finance (DeFi)." BIS Working Paper 1066, January 2023 (DeFi stack taxonomy; Terra/UST Curve pool run case study). <https://www.bis.org/publ/work1066.htm>
- Li, Ye, Stephen Meyer, and Andrei Zlate. "Runs and Flights to Safety: Are Stablecoins the New Money Market Funds?" Federal Reserve Bank of Boston Research Series SRA 2302, June 2023 (Terra 2022 and USDC/SVB 2023 runs; flight-to-safety within stablecoin spectrum). <https://www.bostonfed.org/publications/research-special/2023/runs-and-flights-to-safety-are-stablecoins-the-new-money-market-funds>
- Bullmann, Dirk, Jonas Klemm, and Andrea Pinna. "In search for stability in crypto-assets: are stablecoins the solution?" ECB Occasional Paper Series 230, August 2019 (three-dimensional classification by issuer accountability, decentralization of responsibility, and collateral; trade-off between algorithmic "innovativeness" and peg capacity). <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf>
- Grobys, Klaus, Juha Juntila, James W. Kolari, and Niranjana Sapkota. "On the stability of stablecoins." *Journal of Empirical Finance* 64(C), December 2021, pp. 207–223 (multi-stablecoin peg-deviation panel; fiat-collateralized volatility below algorithmic). <https://doi.org/10.1016/j.jempfin.2021.09.002>
- Brauneis, Alexander, et al. "How stable are stablecoins?" *European Journal of Finance* 30(9), 2024, pp. 1027–1058 (peg deviation and OTC/on-chain depth; δ amplifies in thin markets). <https://doi.org/10.1080/1351847X.2023.2240254>
- Gadzinski, Gregory, Alessio Castello, Vito Liuzzi, and Patrice Sargenti. "Break a peg! A study of stablecoin co-instability." *International Review of Financial Analysis* 96, November 2024, article 103608 (in Terra/LUNA and IRON/TITAN events, algorithmic types were primary shock receivers; fiat-collateralized and crypto over-collateralized CDPs were more resilient after shocks). <https://doi.org/10.1016/j.irfa.2024.103608>
- MakerDAO. "Endgame: The Next Phase of MakerDAO." Litepaper, March 2023 (SubDAO split, MKR governance-token restructuring, post-Black Thursday liquidity-module evolution). Source: official Litepaper v1; not independently audited. <https://endgame.makerdao.com/>
- Congressional Research Service. *Crash of the TerraUSD Stablecoin: Background and Policy Issues*. Insight IN11928, May 18, 2022 (UST/LUNA dual-token arbitrage mechanism; congressional post-mortem of depeg to \$0.12). https://www.congress.gov/crs_external_products/IN/PDF/IN11928/IN11928.1.pdf
- Arner, Douglas W., Raphael Auer, and Jon Frost. "Stablecoins: risks, potential and regulation." *Financial Stability Review*, Banco de España, Autumn 2020 (stablecoin run risk, reserve transparency, and regulatory-framework precursor; contrast with BIS CPMI 2022). <https://www.bde.es/ff/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanci>

- Ferraro, Gianni, Kan Li, and Adi Sunderam. "Stable Coins but Thin Markets." Princeton Economics Working Paper No. 1416, October 2022 (revised 2023). Pegs are more fragile when OTC depth is thin; complementary to Lyons & Viswanath-Natraj (2020). <https://www.princeton.edu/~kan/StableCoins.pdf>
- Griffin, John M., and Amin Shams. "Is Bitcoin Really Untethered?" *Journal of Finance* 75(4), August 2020, pp. 1913–1964 (Tether reserve transparency and BTC pricing; empirical precursor to fiat-collateralized stablecoin audit disputes). <https://doi.org/10.1111/jofi.12815>
- Bahaji, Hamza, and Fabio Prat. "Stablecoins, Central Bank Digital Currencies and Cross-Border Payments." ECB Working Paper 2544, November 2021. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2544~7dd2cc491a.en.pdf>
- Aquilina, Matteo, Sirio Aramonte, Patrick Bisias, Andreas Schrimpf, and Alexander Kothe. "The market structure of stablecoins." *BIS Bulletin* No. 73, 7 February 2023 (issuance concentration, reserve types, and run contagion). <https://www.bis.org/pub/bisbull73.htm>
- Financial Stability Board. "High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements." Final report, July 2023 (GSC classification, reserve assets, and redemption rights). <https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements/>
- Makarov, Igor, and Antoinette Schoar. "Trading and Arbitrage in Cryptocurrency Markets." *Journal of Financial Economics* 135, 2020, pp. 293–319 (cross-exchange arbitrage, peg deviation, and OTC depth). <https://doi.org/10.1016/j.jfineco.2019.08.012>
- Eichengreen, Barry, Poonam Gupta, and Oliver Masucci. "Stablecoins and Emerging Market Cross-Border Payments." IMF Working Paper 23/110, May 2023 (stablecoin adoption in high-inflation corridors and regulatory tension). <https://www.imf.org/en/Publications/WP/Issues/2023/05/05/Stablecoins-and-Emerging-Market-Cross-Border-Payments-534000>
- Catalini, Christian, Alon Goren, and Divya Shah. "Some Simple Economics of Stablecoins." MIT Sloan Research Paper, November 2021 (revised 2022). Mechanism taxonomy: fiat-collateralized, crypto over-collateralized, algorithmic; conditions for unsustainable subsidies. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968382
- MakerDAO. "Direct Deposit Module (D3M): Technical Documentation." 2021–2022 (post-Black Thursday external liquidity module; source: official technical documentation; not independently audited). <https://docs.makerdao.com/smart-contract-modules/d3m-module>
- World Bank. *Migration and Development Brief* 37, December 2023, Box 1.2 (remittances, stablecoin corridors, adoption in fragile corridors). <https://www.knomad.org/publication/migration-and-development-brief-37>
- He, Dong, Ross Leckow, Tommaso Mancini-Griffoli, and Hiroshi Nagaoka. "Stablecoins and the Future of Money." IMF Fintech Notes 2023/001, January 2023 (mechanism spectrum, run risk, and policy framework). <https://www.imf.org/en/Publications/fintech-notes/Issues/2023/01/10/Stablecoins-and-the-Future-of-Money-527630>

Primary Sources, Distributional Effects, and Agent/DePIN Frontiers

Round 53 (mod 6 = 5) adds Cantillon, Buchanan, Buterin/Szabo primary texts, and checkable sources for x402/AgentKit/ERC-4337 and DePIN. Round 64 (mod 6 = 4) adds the Nakamoto–Back–Szabo idea chain,

Lightning, Render/io.net/Helium, and agentic commerce (AP2/TAP/Agent Pay); key citations add chapter/page numbers.

- Cantillon, Richard. *An Essay on Economic Theory (Essai sur la Nature du Commerce en Général)*. c. 1730. English trans., Liberty Fund, 2010. Ch. 7, Part 2 (monetary expansion; non-uniform injection; Cantillon effect). <https://oll.libertyfund.org/titles/cantillon-an-essay-on-economic-theory>
- Buchanan, James M., and Richard E. Wagner. *Democracy in Deficit*. Academic Press, 1977. Ch. 1–2 (Keynesian policy bias under democratic incentives), Ch. 4 (systematic deficit bias). <https://doi.org/10.1016/B978-0-12-139250-3.50008-5>
- Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." Ethereum White Paper, 2014 (rev.). Source: official white paper; not independently audited. <https://ethereum.org/en/whitepaper/>
- Szabo, Nick. "Smart Contracts." 1994. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.k>
- Szabo, Nick. "Formalizing and Securing Relationships on Public Networks." *First Monday* 2(9), September 1997. <https://firstmonday.org/ojs/index.php/fm/article/view/548>
- Szabo, Nick. "Shelling Out: The Origins of Money." 2002. <https://nakamotoinstitute.org/shelling-out/>
- Ethereum Improvement Proposals. EIP-4337: "Account Abstraction Using Alt Mempool." Final, March 2023. <https://eips.ethereum.org/EIPS/eip-4337>
- Coinbase. "x402: HTTP-native micropayments." Protocol specification, May 2025; x402 Foundation launch, September 2025. Source: official protocol documentation; not independently audited. <https://x402.org/>
- Coinbase Developer Platform. "AgentKit: AI agents onchain." Product documentation, November 2024. Source: official documentation; not independently audited. <https://docs.cdp.coinbase.com/agentkit/docs/welcome>
- Akash Network. "Akash Network Whitepaper." 2020 (rev.). Source: official white paper; not independently audited. <https://akash.network/docs/akash-whitepaper/>
- Bittensor. "Bittensor: A Peer-to-Peer Intelligence Market." Whitepaper, 2021. Source: official white paper; not independently audited. <https://bittensor.com/whitepaper>
- Ballandies, Mark, et al. "A Taxonomy for Blockchain-based Decentralized Physical Infrastructure Networks (DePIN)." *Frontiers in Blockchain* 6, 2023, 1272380. <https://doi.org/10.3389/fbloc.2023.1272380>
- Mohan, Deepak. "Decentralized Physical Infrastructure Networks (DePIN)." Messari Research, June 2023. <https://messari.io/report/decentralized-physical-infrastructure-networks-depin>
- Weyl, Eric Glen, Puja Ohlhaber, and Vitalik Buterin. "Decentralized Society: Finding Web3's Soul." *SSRN*, May 2022 (soulbound tokens, on-chain reputation). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
- Sablier Finance. "Sablier: Token streaming protocol." Documentation, 2024. <https://docs.sablier.com/>
- Superfluid. "Superfluid: Money streaming protocol." Documentation, 2024. <https://docs.superfluid.finance/>
- Back, Adam. "Hashcash - A Denial of Service Counter-Measure." August 2002. §1–3 (proof of work and verifiable cost). <http://www.hashcash.org/papers/hashcash.pdf>

- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." October 2008, §2–4 (timestamp server, PoW citing Hashcash, longest-chain rule). See S–Z section above; <https://bitcoin.org/bitcoin.pdf>
- Szabo, Nick. "Trusted Third Parties Are Security Holes." May 1999. <https://nakamotoinstitute.org/trusted-third-parties/>
- Szabo, Nick. "Secure Property Titles with Owner Authority." 1998. <https://nakamotoinstitute.org/secure-property-titles/>
- Buterin, Vitalik. "Notes on Blockchain Governance." December 17, 2017. <https://vitalik.ca/general/2017/12/17/voting.html>
- Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." White Paper, 2014, §"Ethereum Accounts" / "Applications" (Turing-complete state machine). See above; source: official white paper; not independently audited.
- Poon, Joseph, and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." Draft v0.5, 2016. <https://lightning.network/lightning-network-paper.pdf>
- Render Network Foundation. *Render Network Whitepaper* v4.0. Originally posted August 28, 2017; updated May 26, 2023. Source: official white paper v4.0; not independently audited. <https://renderfoundation.com/whitepaper>
- io.net. "Company Origins & Documentation." 2023–2025 (DePIN GPU aggregation, Ray orchestration, Solana settlement). Source: official documentation; not independently audited. <https://io.net/docs/guides/inception>
- Helium Foundation. "Helium Documentation: Network Overview & Solana Migration." 2023 (IoT/5G DePIN, HNT/IOT/MOBILE tokens, 2023-04-18 Solana migration). Source: official documentation; not independently audited. <https://docs.helium.com/>
- Haleem, Amir, et al. "Helium: A Decentralized Wireless Network." White Paper, 2018. Source: official white paper; not independently audited. Internet Archive: <https://web.archive.org/web/20200328171442/https://helium.com/whitepaper>
- Google. "Agent Payments Protocol (AP2)." Technical specification, September 2025. Source: official protocol documentation; not independently audited. <https://github.com/google-agentic-commerce/AP2> ; Spec site: <https://google-agentic-commerce.github.io/AP2/>
- Google Cloud. "Announcing Agent Payments Protocol (AP2)." Blog, September 16, 2025. <https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol>
- Visa Inc. "Trusted Agent Protocol (TAP)." Developer documentation & RFC 9421 message signatures, 2025 pilot. Source: official documentation; not independently audited. <https://developer.visa.com/capabilities/trusted-agent-protocol> ; <https://github.com/visa/trusted-agent-protocol>
- Mastercard. "Mastercard unveils Agent Pay." Press release, April 29, 2025 (Agentic Tokens, Know Your Agent). Source: official press release; not independently audited. <https://newsroom.mastercard.com/news/press/2025/april/mastercard-unveils-agent-pay-pioneering-agentic-payments-technology-to-power-commerce-in-the-age-of-ai/>
- Szabo, Nick. "Money, Blockchains, and Social Scalability." *Unenumerated*, February 2017 (social scalability: verifiable rules replace interpersonal trust costs; aligned with this book's second dimension of

"verifiability"). <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>

- Szabo, Nick. "Secure Property Titles with Owner Authority." 1998 (distributed property title registration and timestamp chains; precursor to bit gold steps 4–6). <https://nakamotoinstitute.org/secure-property-titles/>
- Finney, Hal. "Reusable Proofs of Work (RPOW)." 2004 (engineering middle link for bit gold; transparent server + remote attestation). <https://nakamotoinstitute.org/library/finney-rpow/>
- Wood, Gavin. "Ethereum: A Secure Decentralised Generalised Transaction Ledger." Yellow Paper, 2014 (rev. 2022). §1–2 (state-transition system); §4.2 (Gas and execution metering); §7 (contract creation). <https://ethereum.github.io/yellowpaper/paper.pdf>
- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016. Ch. 1–3 (P2P ledgers, consensus, wallets and keys). <https://bitcoinbook.cs.princeton.edu/>
- Ethereum Improvement Proposals. EIP-20: "Token Standard." Final, November 2015 (ERC-20 interface semantics: transfer/approve/balanceOf). <https://eips.ethereum.org/EIPS/eip-20>
- Protocol Labs. "Filecoin: A Decentralized Storage Network." Whitepaper, 2017 (rev. 2022). Source: official white paper; not independently audited (storage-type DePIN; Proof-of-Replication + proof of spacetime). <https://filecoin.io/filecoin.pdf>
- Cloudflare & Coinbase. "Launching the x402 Foundation with Coinbase, and support for x402 transactions." Blog, September 23, 2025 (HTTP 402 micropayments and Agent settlement ecosystem). <https://blog.cloudflare.com/x402/>
- Coinbase. "x402: The Payment Protocol for Agentic Commerce." Whitepaper, 2025. Source: official white paper; not independently audited. <https://www.x402.org/x402-whitepaper.pdf>
- Stripe. "Agentic Commerce API." Product documentation, 2025. Source: official documentation; not independently audited. <https://docs.stripe.com/agentic-commerce>
- GS1. "EPCIS 2.0 — Core Business Vocabulary (CBV) and EPCIS 2.0 Standard." 2024 revision (logistics event capture and Digital Link linkage). <https://www.gs1.org/standards/epcis>
- IETF. Ryan, Mark, et al. "The Payment HTTP Authentication Scheme." Internet-Draft draft-ryan-httpauth-payment-00, 2025 (Machine Payments Protocol / MPP core draft; standardizing HTTP 402 semantics). <https://datatracker.ietf.org/doc/draft-ryan-httpauth-payment/>
- IETF. Jones, M., et al. "HTTP Message Signatures." RFC 9421, February 2024 (message-signature basis for Agent authentication such as Visa TAP). <https://www.rfc-editor.org/rfc/rfc9421.html>
- ISO/IEC JTC 1/SC 41. ISO/IEC TR 30166:2020 — *Industrial IoT — Reference architecture and common requirements* (industrial IoT reference architecture; contrast with ch23 §2 M2M). <https://www.iso.org/standard/53211.html>
- ISO. ISO/NP 23485 — *Consumer protection — Privacy by design for consumer goods and services* (new project rejected in 2018; not an M2M payment standard—ch23 §2 citations must distinguish from GS1 EPCIS / IETF MPP). <https://www.iso.org/standard/74044.html>

Work	Dialogue point	Main chapters
Szabo (2017) social scalability	Verifiable rules replace interpersonal trust	ch06 §4, ch07 §6, ch20 §9

Work	Dialogue point	Main chapters
Finney (2004) RPOW	bit gold → Bitcoin engineering bridge	ch06 §1, ch14 §6, appendix bit-gold
Wood (2014/2022) Yellow Paper §1–4	Ethereum state machine and Gas	ch06 §2, ch12 §8
Narayanan et al. (2016) Princeton	Textbook-grade P2P ledger survey	ch06 §1, ch12 §5
EIP-20 / ERC-20	Token standard interface	ch12 §8
Filecoin (2017/2022)	Storage-type DePIN	ch23 §3
x402 Whitepaper + Cloudflare (2025)	Agent HTTP micropayments	ch20 §10, ch21 §2
IETF MPP draft (2025)	M2M HTTP 402 standardization	ch23 §2
RFC 9421	Agent message signatures (Visa TAP)	ch20 §10, ch22 §7
GS1 EPCIS 2.0 (2024)	Logistics events—payment triggers	ch23 §2

- Wei Dai. "b-money." February 1998 (distributed ledgers, proof of work, and anonymous participants; acknowledged in Satoshi Nakamoto Bitcoin white paper References). <https://www.weidai.com/bmoney.txt>
- Szabo, Nick. "The God Protocol." 1997 (verifiable third-party substitution: "God knows the outcome; humans can only verify"—institutional precursor to smart contracts and bit gold). <https://nakamotoinstitute.org/the-god-protocol/>
- Szabo, Nick. "Shelling Out: The Origins of Money." 2002 (prehistoric collectibles cooperation and origins of monetary coordination; read with Menger saleability emergence). <https://nakamotoinstitute.org/shelling-out/>
- Easley, David, Maureen O'Hara, and Soumya Basu. "From mining to markets: The evolution of bitcoin transaction fees." *Journal of Financial Economics* 169, 2025, pp. 103892 (after block-reward decline, fee markets become the main miner-incentive channel; evolution from P2P ledger to market pricing). <https://doi.org/10.1016/j.jfineco.2024.103892>
- Anthropic. "Model Context Protocol Specification." Version 2024-11-05, November 2024 (JSON-RPC semantics for Agent tool calls; orchestration layer separated from settlement layer). <https://spec.modelcontextprotocol.io/specification/2024-11-05/>
- Google. "Agent2Agent (A2A) Protocol Specification." April 2025 (Agent discovery, task delegation, and capability cards; complementary to AP2 payment-authorization chains). <https://github.com/google/A2A/blob/main/docs/specification.md>
- Buterin, Vitalik. "Ethereum Design Rationale." Wiki, 2014–2015 (account model, Gas metering, state tree, and "world computer" trade-offs; intersects Wood Yellow Paper §§1–4). <https://github.com/ethereum/wiki/wiki/Design-Rationale>
- Buterin, Vitalik. "DAOs, DACs, DAs and More: An Incomplete Terminology Guide." Ethereum Blog, May 6, 2014 (on-chain governance and autonomous-organization terminology; precursor to governance-token lineages). <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide>
- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016. Ch. 3–5 (consensus, mining economics, wallets and keys; textbook-grade Nakamoto mechanism survey). <https://bitcoinbook.cs.princeton.edu/>
- Superfluid. "Superfluid Protocol Documentation." 2024 (f1ow/deleteFlow streaming-payment semantics; contrast with Agent session-lifecycle settlement). <https://docs.superfluid.finance/>
- Sablier Finance. "Sablier V2 Documentation." 2024 (linear/step vesting streams; precedent for per-second M2M release). <https://docs.sablier.com/>

- Friedman, Milton. *A Program for Monetary Stability*. Fordham University Press, 1960. Ch. 4–5 (k% rule constrains an existing central bank; does not advocate abolishing monopoly or opening private competitive currencies). <https://fraser.stlouisfed.org/title/program-monetary-stability-3969>
- Helleiner, Eric. *The Making of National Money: Territorial Currencies in Global History*. Cornell University Press, 2003. Ch. 2 (colonial hut taxes, territorial monetization, and forced circulation; historiography of the tax anchor). Cornell 2003 edition.
- Austin, Gareth, and William Darity Jr. "The Historical Origins of Inflation Targeting." *Journal of Post Keynesian Economics* 29(4), Summer 2007, pp. 635–660 (survey of African colonial hut taxes and forced monetary adoption). <https://doi.org/10.2753/PKE0160-3477290408>
- Fetter, Frank W. *Development of British Monetary Orthodoxy, 1797–1875*. Harvard University Press, 1965. Ch. 7–9 (1844 Bank Charter Act; split of Issue and Banking Departments; crisis suspensions of 1847/1857/1866). Harvard 1965 edition.
- McLeay, Michael, Amar Radia, and Ryland Thomas. "Money Creation in the Modern Economy." *Bank of England Quarterly Bulletin*, 2014 Q1, pp. 14–27 ("banks create deposits when they lend"; breaks the savings-intermediation narrative). <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy>
- Bernanke, Ben S. *The Courage to Act: A Memoir of a Crisis and Its Aftermath*. W.W. Norton, 2015. Ch. 7–9 (2008 crisis response, three rounds of QE, and institutionalization of unconventional tools). Norton 2015 edition.
- Beanstalk Farms. "Post-Mortem: Beanstalk Farms Governance Exploit." April 2022 (flash-loan borrowed governance weight, BIP-18 passage, ~\$182M asset drain; on-chain governance-capture case). <https://beanstalkfarms-almanac.medium.com/beanstalk-farms-governance-exploit-post-mortem-847a8566923e>
- Hayek, F.A. "Competition as a Discovery Procedure." In *New Studies in Philosophy, Politics, Economics and the History of Ideas*, University of Chicago Press, 1978, pp. 179–190 (competition as discovery of dispersed knowledge; footnote style aligned with ch04 §2). University of Chicago Press 1978 edition.
- Financial Accounting Standards Board. Accounting Standards Update No. 2023-08, *Intangibles—Goodwill and Other—Crypto Assets (Subtopic 350-60)*, December 2023 (ASC 350-60: fair-value measurement, changes through earnings; effective fiscal 2025). <https://www.fasb.org/page/document?pdf=ASU+2023-08.pdf>
- Kiyotaki, Nobuhiro, and Randall Wright. "On Money as a Medium of Exchange." *Journal of Political Economy* 97(4), August 1989, pp. 927–954 (saleability ranking under random matching; formal precursor to Menger §§1–2). <https://doi.org/10.1086/261634>
- Kiyotaki, Nobuhiro, and Randall Wright. "A Search-Theoretic Approach to Monetary Economics." *American Economic Review* 83(1), March 1993, pp. 63–77 (intrinsic vs extrinsic saleability; read with Mises regression theorem and Selgin 2015 synthetic commodity money). <https://doi.org/10.1257/aer.83.1.63>

Part VII Strongest Counterarguments (ch24–ch26 Cross-Index)

- State theory of money / tax anchor: Knapp (1924) Ch. 1; Innes (1913/1914); Wray (2012) Ch. 2, 5–6; Brunnermeier & Niepelt (2020) (private/public money equivalence theorem → ch24 §2, ch26 §2)
- Lender of last resort: Bagehot (1873) Ch. 2, 7; Calomiris (1989) (LOLR costs and moral hazard → ch24 §2, ch26 §8); MakerDAO Black Thursday Post Mortem (2020-03-12)
- New Keynesian / 2% target: Woodford (2003) Ch. 6–7; Galí (2015) Ch. 8, 15; Clarida, Galí & Gertler (1999) (→ ch24 §2, ch26 §2/§5); Bernanke et al. (1999) Ch. 1–2; Eggertsson & Woodford (2003); Sargent (1999) *Conquest of American Inflation* Ch. 2–3

- MMT refined / fiscal-monetary game: Wray (2012); Kelton (2020); Sargent & Wallace (1981) (→ ch24 §2, ch25 §1, ch10 §8); Kydland & Prescott (1977) (time inconsistency → ch24 §2, ch26 §5)
- Added in round 138: Brunnermeier & Niepelt (2020) three equivalence conditions; Leeper (1991); Woodford (1996) NBER MA; Rotemberg & Woodford (1997); Friedman (1960) k% rule; MiCA (EU) 2023/1114; Bindseil (2024) OP 322 §5–6

Glossary

Quick reference for this book's core terms.

Figures and Works

Dr. Bright

Pen name of this book's author; completed in 2024. Taking Hayek's *The Denationalization of Money* as a mirror, it discusses the evolution of monetary order in the age of the value internet.

The Popularization of Money

This book's core concept: the creation and choice of value measures need no longer be monopolized behind a few gates; protocol standardization makes issuance rules open, participatory, and composable. The subtitle *A New Chapter in Monetary Civilization: Tribal Tokens • State Fiat • Popular Protocol • Value in Direct Flow* summarizes the civilizational history of coordination scale in four arcs; in intellectual lineage it takes Hayek's *The Denationalization of Money* as a counterpart, without advocating the abolition of exchange and settlement themselves.

Protocol and Asset Standards

PCIM (Public Currency Issuance Mechanism)

An over-collateralized public-domain currency issuance mechanism, also called the "new gold standard"—at the abstract layer: anyone holding agreed volatile collateral may, under open rules, competitively issue public currency pegged to fiat units with over-collateralization, with no single-point issuer. Collateral discipline uses dynamic tiers: circulation thresholds for each mapping trigger governance votes on the mint yield rate σ (inverse of $C_0 = 100\%/\sigma$); if a vote fails, the prior tier is kept; the ordinary upper-tier ceiling is about $\sigma = 61.8\%$, $C_0 \approx 161.8\%$; in a crisis a separate vote may raise C_0 and lower σ to tighten (Chapter 14, Section 2.2). No MakerDAO-style liquidation/warning lines (L/W); stability rests on same-price oracles, mint/redeem arbitrage (ϵ), protocol reserves (R), and tier votes. Full English name: *Public Currency Issuance Mechanism* (not Public Competitive Issuance System).

Implementation example (Openverse): collateral Bitgold (BTG); public standard VRC-10 (Bitcurrency). When listed alongside DAI or USDC, PCIM names the mechanism class; Openverse names a deployment instance.

Mint yield rate σ (VRC-10)

The share of Bitgold market value that may be minted as Bitcurrency face value per unit of collateral; $\sigma = 100\%/C_0$. Set by circulation tiers and governance votes, not a fixed constant. Bitcurrency-USD reference tiers: votes triggered at 1M / 10M / 100M / 1B USD circulation, deliberating σ of 23.6%, 38.2%, 50%, 61.8% respectively (other mappings may configure different thresholds).

Circulation-tier governance vote (VRC-10)

Each VRC-10 mapping triggers dynamic-ratio votes by on-chain circulation S for that mapping; if passed, switch to the deliberated tier; if rejected, the collateral ratio is unchanged. In crisis, votes may raise the collateral ratio (lower yield rate). VRC-10 only; VRC-11 does not participate.

$C(x)$ (post-shock collateral ratio)

After BTG falls x relative to the oracle reference price, the collateral ratio of an isomorphic position: $C(x) = C_0(1 - x)$. C_0 is the currently effective tier collateral ratio; at the upper tier $C_0 \approx 161.8\%$, $x^* \approx 38.2\%$ is the critical drawdown at which coverage falls below 100%.

x^* (critical coverage drawdown, VRC-10)

The critical drawdown of Bitgold relative to the oracle reference price at which isomorphic-position collateral ratio $C(x) = C_0(1 - x)$ falls below 100%: $x^* = 1 - 100\%/C_0$. At the upper tier $C_0 \approx 161.8\%$, $x^* \approx 38.2\%$ —not a stake share, but a BTG price-shock threshold.

Oracle (PCIM)

Minting and redemption read the same on-chain TWAP (e.g. 1-hour window) plus a redundant median; if single-block price deviation exceeds threshold θ , circuit-break—pause new minting while allowing top-up collateral and redemption.

Arbitrage bandwidth ε

The sum of fees, slippage, and delay on mint/redeem channels; when $x < x^*$, the upper bound on peg deviation is $\delta \leq \varepsilon$. Usually designed to be $< 1\%$.

Peg deviation δ

The proportional deviation of Bitcurrency's secondary-market price from its nominal peg unit (e.g. 1 dollar) (e.g. $\delta = 0.03$ means 3% off-peg). The PCIM minimal model gives an upper bound on δ : when $x < x^*$, $\delta \leq \varepsilon$; when $x \geq x^*$, $\delta \leq \varepsilon + \max(0, g(x) - R)$.

Liquidation line L / warning line W

Typical MakerDAO/CDP parameters: forced auction when collateral ratio C breaches L ; warning near W . Neither VRC-10 nor VRC-11 sets L/W ; $C(x)$ is used only to monitor coverage and as circuit-breaker input, and does not trigger on-chain forced auctions—under extreme stress the pressure path is redemption runs and reserve drawdown (public domain) or off-chain redemption runs (private domain), not Maker-style liquidation cascades. VRC-12 (Bitsecurity) may retain independent liquidation thresholds; do not conflate with VRC-10/11.

Collateral gap $g(x)$

The shortfall of on-chain hard collateral relative to debt face value after BTG falls $x\%$: $g(x) = \max(0, (100\% - C(x))/100\%)$. When $x \geq x^*$, peg pressure moves with $g(x) - R$ (reserve R). For VRC-11, from the first mint $g(0) = 100\% - C_0 = 38.2\%$ (a structural gap, not requiring BTG to fall 38.2% before it appears); contrast with x^* under "two kinds of 38.2%" below.

Protocol reserve R

Protocol reserves as a share of circulating Bitcurrency; when $x \geq x^*$ they can absorb the collateral gap so that peg-deviation upper bound $\delta \leq \varepsilon + \max(0, g(x) - R)$.

Two kinds of 38.2% (do not conflate)

(1) $x^* \approx 38.2\%$: under VRC-10 upper-tier over-collateralization, BTG's critical drawdown—the price-shock threshold at which coverage falls below 100%; upper-tier stake ratio about 161.8%, with 61.8% as excess buffer. (2) $g(0) = 38.2\%$: VRC-11 under-collateralization's structural gap—from the first mint, on-chain hard collateral is already 38.2 percentage points short of face value. The numbers coincide with the golden ratio; the meanings are entirely different.

Over-collateralization / 61.8% excess buffer (VRC-10)

161.8% stake ratio (upper tier)

On the VRC-10 ordinary up-tier path's upper tier: at mint yield $\sigma = 61.8\%$, minting 100 of Bitcurrency requires staking about 161.8 of Bitgold. Lower-circulation tiers are higher and more conservative (see circulation-tier governance votes). Applies only to the VRC-10 / PCIM public layer.

Under-collateralization / 61.8% stake ratio (VRC-11)

Minting 100 of Privcurrency requires staking about 61.8 of Bitgold—a 61.8% stake ratio. This is under-collateralization—collateral value below face value issued—forming a golden-ratio contrast with VRC-10's upper-tier ~161.8% over-collateralization ($\varphi^{-1} \approx 0.618$). Private-domain stability must layer enterprise reputation, whitelist constraints, and off-chain redemption; on-chain hard collateral alone cannot close the peg.

No liquidation line / no warning line (VRC-10 / VRC-11)

VRC-10 and VRC-11 neither adopt MakerDAO/CDP-style liquidation lines (L) or warning lines (W). Position collateral ratio $C = \text{collateral market value} / \text{debt face value}$ is used only to monitor coverage; VRC-10, under currently effective tier over-collateralization, maintains the peg via mint/redeem, circuit-breaker pauses, and reserves; VRC-11, at 61.8% under-collateralization, layers enterprise reputation, whitelists, and off-chain redemption. Other standards such as VRC-12 (Bitsecurity) may retain independent liquidation thresholds; do not conflate with VRC-10/11.

PCIM minimal peg model

Comparative statics under a one-period isomorphic-position framework: post-shock collateral ratio $C(x) = C_0(1 - x)$; critical coverage drawdown $x^* = 1 - 100\% / C_0$ (about 38.2% for VRC-10). When $x < x^*$ and redemption channels work, peg deviation $\delta \leq \varepsilon$ (arbitrage bandwidth); when $x \geq x^*$, gap $g(x) = \max(0, 100\% - C(x))$, $\delta \leq \varepsilon + \max(0, g(x) - R)$ (when reserve R can absorb)—not on-chain forced liquidation. VRC-11 under-collateralization requires separate assessment of off-chain credit risk. The model gives an upper bound on δ , not a promise; given observed δ and x , one can back out which chain—arbitrage, reserve, or oracle—has failed. Three mechanism chains—oracle pricing, over-collateralization constraint, mint/redeem arbitrage—jointly yield the upper-bound function for peg deviation.

PCIM peg theorem (one sentence)

After BTG falls $x\%$, $C(x) = C_0(1 - x)$; when $x < x^*$, $\delta \leq \varepsilon$; when $x \geq x^*$, $\delta \leq \varepsilon + \max(0, g(x) - R)$ —VRC-10 is an over-collateralized CDP (DAI-like), substituting redeem arbitrage + reserves for forced liquidation; at the public layer 38.2% is BTG's critical drawdown x^* , at the private layer a structural gap $g(0)$ —do not conflate. Also called the Bright-PCIM peg bound.

Bright-PCIM peg bound

VRC-10 peg-deviation upper-bound theorem: $C(x) = C_0(1 - x)$; $x < x^* \Rightarrow \delta \leq \varepsilon$; $x \geq x^* \Rightarrow \delta \leq \varepsilon + \max(0, g(x) - R)$. Same formula as "PCIM peg theorem (one sentence)"; given on-chain x and observed δ , back out which of arbitrage, reserve, or oracle has failed. Full English mechanism name: *Public Currency Issuance Mechanism*.

PCIM model variables

Symbol	Meaning	VRC-10 baseline
C_0	Currently effective tier collateral ratio	Upper-tier example 161.8%
x	BTG drawdown vs oracle reference (0–1)	—

Symbol	Meaning	VRC-10 baseline
$C(x)$	Post-shock collateral ratio	$C_0(1 - x)$
x^*	Critical drawdown when coverage falls below 100%	$\approx 38.2\%$
$g(x)$	On-chain collateral gap (share of debt face)	$\max(0, 100\% - C(x))$
ε	Mint/redeem arbitrage bandwidth	Usually $< 1\%$
R	Protocol reserves as share of circulation	Scenario assumption
δ	Peg deviation (secondary p vs peg)	Upper bound in Props. 2–3
L/W	Liquidation / warning lines	VRC-10/11 unset
θ	Oracle single-block anomaly circuit-breaker threshold	e.g. 20%

Liquidation mechanism: MakerDAO/DAI triggers on-chain forced auctions when $C < L$ —March 2020 "Black Thursday" showed that liquidation itself can amplify the fall. VRC-10 and VRC-11 neither set L/W ; $C(x)$ is monitoring and circuit-breaker input only and does not trigger on-chain auctions. Under extreme markets the pressure path is redemption run + reserve drawdown (public) or off-chain redemption run (private), not Maker-style cascade liquidation. VRC-12 (Bitsecurity) retains independent CDP liquidation thresholds—securities-layer risk is separate; do not conflate with PCIM public/private domains.

Three-chain closure (VRC-10 peg architecture)

The PCIM peg closes jointly through three chains; none is dispensable: (1) oracle chain—mint/redeem read the same TWAP + redundant median + anomaly circuit-breaker; (2) collateral chain— C_0 is the current tier (must be $> 100\%$ for over-collateralization), no L/W ; (3) arbitrage chain—when $x < x^*$, mint/redeem constrain p to $[1 - \varepsilon, 1 + \varepsilon]$.

VRC-10 / Bitcurrency

Public-domain currency standard. Competitively issued via Bitgold dynamic-tier over-collateralization, pegged to ISO 4217 fiat units (upper-tier stake ratio about 161.8%), for cross-ecosystem stable settlement. Global primary circulating media means VRC-10 only, not VRC-11 Privcurrency.

Exit of inferior money

Under parallel competition without forced parity, fiat with mismanaged monetary policy and its on-chain mappings lose C-money functions (cross-border settlement, open-ecosystem pricing, long-term store of value) because holders, merchants, and protocol routers do not voluntarily choose them—"bad money drives out bad money" in the literal competitive sense, not Gresham's forced-parity mechanism. Exit is functional marginalization, not the physical disappearance of symbols or domestic legal tender.

Reserve—circulation division of labor

Functional layering of public C-money: the reserve layer is fixed-supply Bitgold (BTG), unified collateral and POS stake; the circulation layer is a few (not pre-assigned by nationality) VRC-10 Bitcurrencies, carrying dynamic global medium and unit-of-account roles. Reserves should be "one"; circulation should be "few."

VRC-11 / Privcurrency

Private-domain stablecoin standard. For enterprises or closed trade circles, minted with Bitgold under-collateralization (61.8% stake ratio); permissioned whitelist circulation; names such as StarUSD, MicroUSD.

VRC-12 / Bitsecurity

Equity-type token standard. Enterprises stake Bitgold to issue; may map real-world assets (RWA) on-chain.

Bitgold (BTG)

Openverse native standard asset; total supply about 200 million, with roughly three-year halvings. As PCIM collateral, POS stake, and fee carrier, it underpins public- and private-domain currency issuance.

bit gold (Szabo's conception)

Nick Szabo's 2005 conception of online "bit gold" with verifiable scarcity: proof of work creates unforgeable scarce bits, distributed property title registration, and timestamp chains—a precursor to Bitcoin ideas; 1997's "The God Protocol" is a precursor to verifiable third-party substitution; 1999's "Trusted Third Parties Are Security Holes" is its institutional corollary; Finney's 2004 RPOW is an engineering middle step; 2017's "social scalability" aligns with this book's second dimension of "verifiability"; this book's appendix includes the bit gold original.

b-money (Wei Dai's conception)

Wei Dai's 1998 conception of distributed ledgers and proof of work; acknowledged in the References of Satoshi Nakamoto's Bitcoin white paper. A precursor link in the Nakamoto–Back–Szabo idea chain.

The God Protocol

Nick Szabo's 1997 concept: "God knows the outcome; humans can only verify"—an institutional precursor to verifiable third-party substitution, in the same lineage as bit gold and smart contracts.

Hashcash

Adam Back's 2002 proof-of-work mechanism against spam; Satoshi Nakamoto's Bitcoin white paper §4 embeds it in monetary issuance discipline.

RPOW (Reusable Proofs of Work)

Hal Finney's 2004 engineering prototype based on bit gold ideas: transparent server + remote attestation to verify work—a middle link between Szabo's conception and Nakamoto's chained ledger.

social scalability

Nick Szabo's 2017 concept: blockchain money's value lies in replacing interpersonal trust costs with verifiable rules, so strangers can collaborate without knowing each other—aligned with this book's second emergent dimension of "verifiability."

Filecoin (FIL)

Protocol Labs' decentralized storage network (storage-type DePIN), organizing storage delivery with Proof-of-Replication and proof of spacetime, with FIL incentivizing nodes.

Openverse (Layer 0, value-exchange layer)

Openverse is designed as Layer 0—a globally decentralized value-exchange layer: at the protocol layer it provides POS consensus, final-settlement anchoring, Bitgold staking, PCIM public issuance, VTP value routing, and cross-domain interoperability, so that Ethereum, Cosmos chains, consortium chains, and in-ecosystem application chains and other Layer 1 networks can all connect. In white-paper engineering terms, Hub Chain corresponds to the Layer 0 core chain (consensus and clearing anchor, not hosting application smart contracts); Zones correspond to native Layer 1 application chains within the ecosystem—an implementation layering, not the full architectural boundary.

VTP (Value Transfer Protocol)

The routing protocol of Openverse's Layer 0 value-exchange layer, analogous to HTTP for information networks, responsible for cross-chain and cross-Layer 1 value addressing, transfer, and finality confirmation.

DeFi Stability Mechanisms and Comparative Terms

CDP (Collateralized Debt Position)

An on-chain over-collateralized lending position: users lock crypto assets and borrow stablecoins at a collateral ratio; forced auction when the ratio breaches the liquidation line (typical MakerDAO/DAI design). VRC-10 belongs to the CDP family on the over-collateralization dimension but sets no liquidation/warning lines.

DAI

MakerDAO's decentralized over-collateralized stablecoin, collateralized by ETH and other on-chain assets, with parameters adjusted via liquidation lines and on-chain governance. PCIM/Bitcurrency belongs to the same over-collateralized CDP family in mechanism lineage, but with different parameters and risk paths.

Anchor Protocol

High-yield deposit protocol in the Terra/UST ecosystem; ~20% UST deposit APY subsidized by ANC token inflation (source: official white paper; not independently audited). When subsidies prove unsustainable, large holders exit first, compounding the UST death spiral.

Reserve redeemability

Lyons & Viswanath-Natraj (2020) framework: stablecoin pegs depend not only on reserve statements but on whether holders can redeem at face value in time; pegs are more fragile when OTC depth is thin. Ferraro, Kan & Sunderam (2022) add a "thin markets" dimension.

sophisticated-first exit

Liu, Makarov & Schoar (2023) on-chain evidence: in early UST depeg, large, high-information participants exited before retail; timing aligns with Anchor high-yield subsidies becoming unsustainable.

Algorithmic vs over-collateralized (stability-mechanism spectrum)

Ortiz & Witte (2023) ex-post comparison: algorithmic stablecoins (e.g. UST) redeem significantly faster under stress than over-collateralized CDPs (e.g. DAI)—the former are "confidence-collapse runs," the latter "collateral-shrinkage runs." Bullmann, Klemm & Pinna (2019) ECB three-dimensional classification (issuer accountability, decentralization of responsibility, collateral) further shows a systematic trade-off between algorithmic "innovativeness" and peg capacity. Assessment must classify first; do not conflate.

Co-instability

Gadzinski et al. (2024) structural-break and co-occurrence analysis of a multi-stablecoin panel: in Terra/LUNA, IRON/TITAN and similar events, algorithmic types were the primary receivers of shocks; fiat-collateralized and crypto over-collateralized CDPs were relatively more resilient after shocks—read separately from single-protocol TVL narratives.

Maker Endgame

MakerDAO's 2023 protocol-restructuring plan: split Maker into SubDAOs, restructure the MKR governance token, and continue post-Black Thursday evolution of liquidity modules such as D3M. Source: official Endgame Litepaper v1; not independently audited.

Algorithmic stablecoin

Pegs maintained mainly via dual-token burn/mint, algorithmic balance-sheet expansion, or high-yield subsidies, rather than hard collateral coverage consistently above 100%. Terra/UST (2022 collapse) is the canonical counterexample.

Death spiral

Under depeg pressure, an algorithmic stablecoin absorbs stablecoin supply by minting more of its native coin, further depressing the native price and deepening the depeg in a self-reinforcing loop. The 2022 UST/LUNA collapse is the landmark case.

Black Thursday

12 March 2020 ETH crash triggering MakerDAO liquidation spirals, zero-bid auctions, and DAI premium; the same day the Fed injected large liquidity. A comparative case of protocol money lacking a lender-of-last-resort function.

Verifiability

The second dimension of monetary emergence in the digital age (alongside Menger's "saleability"): whether rule execution, on-chain state, and history can be independently checked at low cost by any third party (including programs). Szabo (2017) "social scalability" states the same requirement from an institutional-collaboration angle.

Saleability

Core concept in Menger's origin-of-money theory: goods gain advantage as media of exchange by being more divisible, portable, and widely demanded; paired with verifiability.

CBDC and Digital Sovereignty

CBDC (Central Bank Digital Currency)

The digital form of central-bank liabilities, split into **wholesale** (inter-institution clearing) and **retail** (facing the public). BIS 2020 seven-central-bank principles position it as a digital extension of cash, not a replacement for commercial-bank credit intermediation.

Retail / wholesale CBDC

Retail CBDC faces individuals and firms directly and may trigger deposit disintermediation; wholesale CBDC upgrades the interbank final-settlement layer with limited public impact—Carapella & Fleischman (2020) position it as payments-system innovation, far less politically contested than retail disintermediation. Niepelt (2024) aligns the taxonomy with policy questions such as "can the public redeem public money at face value" and "can non-banks access central-bank liabilities."

Deposit disintermediation

The public shifts commercial-bank deposits into CBDC (direct central-bank liability, no counterparty risk), compressing banks' credit-creation base. Bindseil (2024) and Auer et al. (2022) note that shock size depends heavily on whether CBDC pays interest and whether holding caps apply—with zero interest and roughly €3,000 per-person caps, euro-area absorption is on the order of trillions of euros.

Payment-type / investment-type CBDC (Bindseil layering)

Payment-type CBDC is non-interest-bearing with holding caps, mainly a cash extension; investment-type CBDC pays interest, may strengthen policy-rate pass-through to bank liabilities, but also hardens the zero lower

bound. The ECB digital-euro legislative draft leans toward payment-type design.

Tiered CBDC

Bindseil (2020) interest-tiering design: everyday payment balances keep zero or very low rates; holdings above a threshold face lower (even negative) CBDC rates, making CBDC marginally inferior to bank deposits and limiting disintermediation incentives.

Tiered privacy

Bindseil and Panetta (2021) privacy–compliance compromise for retail CBDC: small-value offline anonymity, large-value online auditability—alongside holding caps and waterfall mechanisms in the digital-euro legislative draft as control devices.

Waterfall mechanism

Companion to holding caps in the digital-euro legislative draft: excess CBDC balances automatically transfer back to bank accounts, preventing CBDC from becoming a store-of-value asset competing with government bonds. Kumhof & Noone (2021) list it among financial-stability design principles.

Unified ledger

BIS (2023) *The Future Monetary System* vision of programmable financial infrastructure: wholesale CBDC, tokenized deposits, and on-chain assets settle atomically on the same stack—not replacing banks with CBDC, but juxtaposing the final-settlement layer with a composable contract layer.

mBridge

BIS-led multilateral wholesale CBDC platform (Hong Kong SAR, Thailand, UAE, mainland China, and others), entering MVP in 2024, targeting cross-border PvP atomic settlement. Functionally overlaps on-chain stablecoins in remittance use cases; diverges on compliance and sovereign control.

Brunnermeier–Niepelt equivalence proposition

Under particular fiscal–central-bank coordination and frictionless assumptions, introducing CBDC can be equivalent to "central bank direct liability to the public + corresponding adjustment of the banking system," theoretically leaving the monetary-policy stance unchanged; once deposits flee into CBDC in a crisis, or CBDC pays interest without holding caps, the equivalence conditions fail.

Distributional Effects and Political Economy

Cantillon effect

Newly created money is distributed non-uniformly along injection paths: agents near the issuance channel gain purchasing power first; distal agents feel the increase only after prices rise, by which time new purchasing power has already been diluted by first movers. Cantillon (c. 1730) Ch. 7; contemporary QE distributional evidence.

Democracy in Deficit

Buchanan & Wagner (1977): democratic political incentives raise spending and cut taxes in booms, then stimulate again in recessions, while austerity is politically unpopular—producing a cross-cycle bias toward deficits and monetary expansion.

Agent Economy and M2M Settlement

M2M (Machine-to-Machine settlement)

Value transfer completed by programs under preset rules without step-by-step human approval; granularity down to a single API call or GPU-second intervals.

x402

HTTP 402 micropayment protocol (2025): server returns **PAYMENT-REQUIRED**; client Agent signs and retries with **PAYMENT-SIGNATURE**; facilitator completes on-chain stablecoin settlement. Constraint carrier is facilitator reputation.

MCP (Model Context Protocol)

Anthropic's Nov 2024 Agent tool-orchestration standard: `tools/list/tools/call` under JSON-RPC semantics standardize tool calls; orchestration layer separated from settlement layer—payments must close separately via x402/AP2 and the like.

A2A (Agent2Agent)

Google's 2025 standard for Agent discovery, task delegation, and capability cards; complementary to AP2 payment-authorization chains.

AgentKit

Coinbase Developer Platform (Nov 2024) on-chain toolkit for Agents: framework-agnostic action providers, integrated with x402 for autonomous payment; custodial wallets reintroduce reputation constraints.

AP2 (Agent Payments Protocol)

Google's 2025 open Agent payment standard: Verifiable Credentials and Intent/Cart/Payment Mandates build an auditable authorization chain, extending A2A/MCP; constraint carriers are mandate signatures and issuer risk controls.

TAP (Trusted Agent Protocol)

Visa 2025 pilot: based on RFC 9421 HTTP message signatures, letting merchants cryptographically verify Agent identity and authorization; constraint carriers are card-network registration and public-key registries.

Agent Pay (Mastercard)

Mastercard's April 2025 agentic commerce offering: Agentic Tokens bind Agent identity and session limits (Know Your Agent); constraint carriers are card-network tokenization and issuer risk controls.

Lightning Network

Poon & Dryja (2016) Bitcoin off-chain payment-channel network, easing BTC main-chain throughput and micropayment friction; settlement still anchors to volatile BTC.

ERC-4337 / Account Abstraction

Ethereum account-abstraction standard: smart-contract wallets express spending rules in code (whitelists, limits, session keys); Agents submit "intents" that contracts adjudicate and execute.

DePIN (Decentralized Physical Infrastructure Networks)

On-chain order books and stake-slash organize trade in physical resources such as compute, bandwidth, storage, and wireless coverage (Akash, Render, io.net, Helium, Bittensor, and others). Delivery proofs are often

off-chain; pricing often in volatile tokens; taxonomy in Ballandies et al. (2023).

soulbound token

Non-transferable on-chain credentials for Agent/node reputation, permissions, or completion records; conceptual framework in Weyl–Ohlhaver–Buterin (2022).

New Keynesian and Fiscal–Monetary Games

Flexible Inflation Targeting (FIT)

Central banks include both inflation and employment (output) gaps in the reaction function, trading off price stability against real fluctuations; Galí (2015) frames it as the main institutional form of internalizing distributional concerns within a discretionary framework; Taylor (1993) and Clarida–Galí–Gertler (1999) supply empirical benchmarks and formal surveys.

Taylor rule

Taylor's (1993) monetary-policy reaction function: the policy rate should adjust systematically with inflation and output gaps—becoming the empirical benchmark for New Keynesian "science" and many inflation-targeting regimes, between Friedman's $k\%$ fixed rule and pure discretion. Orphanides (2003) shows with historical data that actual policy often systematically departs from the rule-implied path.

Fiscal–monetary active–passive mix (Leeper 1991)

Leeper distinguishes which of monetary and fiscal policy "actively" sets the path and which "passively" accommodates: under "active fiscal, passive monetary" equilibrium, public-debt expansion is more likely to be fulfilled via inflation than tax adjustment—aligned with Sargent–Wallace (1981) unpleasant monetarist arithmetic.

Effective Lower Bound (ELB)

When the nominal policy rate nears zero, further cuts are constrained and the price tool of monetary policy loses force; Woodford (2003) and Eggertsson–Woodford (2003) argue that moderately positive inflation lowers the probability of hitting the ELB and supplies a welfare basis for roughly 2% inflation targets.

unpleasant monetarist arithmetic

Sargent and Wallace (1981): under high fiscal deficits, if the central bank long accommodates fiscal financing at low rates, higher inflation must eventually dilute the debt; programmable interest-bearing CBDC without caps may accelerate that path. Woodford (1996) gives the mirror constraint from public-debt dynamics: long-run price stability requires sufficient discipline on the debt stock. Canzoneri, Cumby, and Diba (2001) state the same logic as a fiscal solvency anchor.

Fiscal dominance

When public debt is large enough that monetary policy must prioritize debt sustainability, a nominally independent central bank is substantively fiscally constrained—rate hikes may trigger a government interest-expense crisis; rate cuts may tolerate inflation. Leeper's (1991) active–passive mix and Canzoneri et al. (2001) fiscal solvency anchor formalize the idea; Bassetto & Messer (2013) discuss contemporary versions under crisis unconventional operations.

Fiscal solvency anchor

Canzoneri, Cumby, and Diba (2001) *AER* 91(5): the long-run price level must be consistent with public-debt solvency; under active-fiscal, passive-monetary equilibrium, inflation becomes the equilibrium outlet for debt

dilution—aligned with Leeper (1991) and Sargent–Wallace (1981). Sims (1994) Fiscal Theory of the Price Level (FTPL) gives a minimal model.

Fiscal Theory of the Price Level (FTPL)

Sims (1994) minimal model: the price level is jointly determined by the fiscal path (tax and debt dynamics) and the monetary-policy regime; when fiscal policy is active, inflation can be an equilibrium adjusting variable. Read with Leeper's active–passive mix.

New Keynesian synthesis

Ball, Mankiw, and Romer (1988) knit nominal rigidities, rational expectations, and policy rules into a unified framework; Woodford (2003) and Galí (2015) develop it into welfare arguments for roughly 2% inflation targets and FIT; Walsh (2017) textbook Ch. 8–11 supplies teachable, estimable operational formulations.

Time inconsistency

Kydland and Prescott (1977): if optimal plans can be revised period by period, policymakers may depart from ex-ante optimal commitments; inflation targeting and operational central-bank independence can be read as institutional responses that strip rate decisions from the electoral cycle.

Good/Bad Competition and Free Banking (Part II)

Gresham's Law

Under legal parity (law-forced fixed exchange rates), overvalued bad money drives out undervalued good money—holders spend bad first and hoard good. Hayek stresses: it applies only under forced parity and must not be called an "inversion" of Thiers' direction under free float; contrast Rolnick–Weber (1986) empirics.

Gresham's Fallacy

Rolnick & Weber (1986) term: statistically alleged "bad drives out good" often fails in free-banking periods without forced parity—when discount is allowed, the direction aligns with Thiers. Mutually corroborating with Hayek's distinction at pp. 42–43.

Thiers' Law

Under free float without forced parity, currencies with continually worsening purchasing power are actively abandoned and relatively stable ones retained—good drives out bad. Argentina, Zimbabwe, Venezuela, and discount-clearing logic in free-banking literature align; Rolnick & Weber (1986) contrast it with Gresham by institutional premise, not as an "inversion" of the same law.

Free Banking

Historical institutional experiments in which private banks competitively issue notes under limited regulation and clear spontaneously. Scotland (1716–1845) and the positive narratives of U.S. economic historians White and Selgin, versus causal doubts from Rockoff, Calomiris, and Kroszner, form a historiographical debate; this book's stance: discipline can be partly endogenized in clearing networks, but depends on gold-standard shadows, lender-of-last-resort expectations, and judicial enforceability—on-chain verifiable rules fill an identification-cost gap; Selgin (1984) evolutionary model and White (1984) option clause appear under free-banking entries in the bibliography.

Option Clause

Liquidity management spontaneously adopted by Scottish free banks: under stress a bank could defer coin redemption of notes for six months while paying compensatory interest (usually 5%). Selgin and White treat it as one endogenous stabilizer of competitive issue; Calomiris questions whether it could operate independently once stripped of the Bank of England lender-of-last-resort shadow. White (1984) ch. 2, pp. 40–52 is a checkable page citation.

Clearinghouse (interbank clearing network)

Multilateral note clearing and discount-reflux mechanisms spontaneously formed by banks in the free-banking era; Timberlake (1984) and Dowd (1993) treat them as institutional embryos of supply discipline endogenized by competitive issue—full nodes on-chain structurally fill the same gap.

Bank Note Reporter

Nineteenth-century U.S. publications by which merchants authenticated and discounted state banknotes; Rockoff (1974) and Dwyer (1996) use their records to analyze wildcat banking and high-information-cost competition.

Wildcat Banking

In the U.S. free-banking era, locating headquarters in remote areas to reduce redemption requests while issuing heavily into distant cities. Dwyer (1996) shows the essence was **arbitrage on authentication and redemption costs**—surface outcomes sometimes resemble Gresham-style retention of inferior notes, but the trigger is information cost, not legal parity.

Par Laws

Legislation forcing notes to be accepted at face value and forbidding discount circulation. Rockoff and Selgin's historiography shows: par laws re-embed Gresham mechanisms in private banking—inferior notes stay in circulation. Structurally isomorphic to incentive distortions of on-chain "forced 1:1 pegs"; Selgin (2010) on the 1865 federal tax suppressing state banknotes.

Institutions and Comparative Concepts

Mint prerogative

The institutional power of a single actor to monopolistically define the unit of account and extract implicit revenue from dilution. This book seeks to dissolve the monopoly of the mint prerogative, not the existence of money as a medium of exchange.

Denationalization of money

Hayek's 1976 claim: abolish the central-bank monopoly of note issue and let private monies compete freely. This book builds on that to discuss protocolized, verifiable contemporary implementation paths.

Value internet

The long-run vision of open standards completing cost reduction and routing for value transfer; VTP, the VRC standard family, and multi-chain interoperability (e.g. IBC) form part of its tech stack.

Bit gold

English introduction

Nick Szabo proposed "bit gold" in 2005 to create *unforgeable scarcity* online, so that stores of value need rely as little as possible on trusted third parties. The core steps are: a public challenge string → compute a proof of work → distributed timestamping → registration on a property title chain → the next bit gold unit takes the previous one as its challenge source. Szabo makes clear that verifying ownership depends on an "unforgeable chain of title," not on mere possession of the bits; assessing value requires inspecting the challenge, the work, and the timestamp; and because of differences in machine architecture, bit gold behaves more like collectibles than fully fungible gold—dealers must bundle units of differing value into larger units of approximately equal value.

This conception directly influenced reusable proofs of work (RPOW) and later Bitcoin design. When reading the original, compare Part IV of this book on battles over standards, proof of work, and third-party trust. The Openverse Bitgold white paper connects Szabo's idea to this book's PCIM mechanism as one engineering realization of that theory. VRC-10 issues Bitcurrency via *dynamic-tier over-collateralization*; VRC-11 mints Privcurrency at 61.8% *under-collateralization* (see Chapter 14, Section 2.2 for the public-domain tier mechanism); neither sets *MakerDAO-style liquidation or warning lines*, and stability rests on *mint/redeem, whitelists, and off-chain credit* (see Chapters 14 and 15 and [glossary.md](#)).

English original

Nick Szabo, December 2005. [Source](#).

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party. Precious metals and collectibles have an *unforgeable scarcity* due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby *unforgeably costly bits* could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function." The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards. Here are the main steps of the bit gold system that I envision:

(1) A public string of bits, the "challenge string," is created (see step 5).

(2) Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

(3) The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

(4) Alice adds the challenge string and the timestamped proof of work string to a distributed property title registry for bit gold. Here, too, no single server is substantially relied on to properly operate the registry.

(5) The last-created string of bit gold provides the challenge bits for the next-created string.

(6) To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

(7) To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp. Note that Alice's control over her bit gold does not depend on her sole possession of the bits, but rather on her lead position in the unforgeable chain of title (chain of digital signatures) in the title registry.

All of this can be automated by software. The main limits to the security of the scheme are how well trust can be distributed in steps (3) and (4), and the problem of machine architecture which will be discussed below.

Hal Finney has implemented a variant of bit gold called RPOW (Reusable Proofs of Work). This relies on publishing the computer code for the "mint," which runs on a remote tamper-evident computer. The purchaser of bit gold can then use remote attestation, which Finney calls the transparent server technique, to verify that a particular number of cycles were actually performed.

The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." (I wrote about this obscurely several years ago.) Thus, it might be possible to be a very low cost producer (by several orders of magnitude) and swamp the market with bit gold. However, since bit gold is timestamped, the time created as well as the mathematical difficulty of the work can be automatically proven. From this, it can usually be inferred what the cost of producing during that time period was. Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items. In this respect "bit gold" acts more like collector's items than like gold. However, the match between this ex post market and the auction determining the initial value might create a very substantial profit for the "bit gold miner" who invents and deploys an optimized computer architecture. Thus, bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today to make commodity markets possible. Trust is still distributed because the estimated values of such bundles can be independently verified by many other parties in a largely or entirely automated fashion.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. The potential for initially hidden supply gluts due to hidden innovations in machine architecture is a potential flaw in bit gold, or at least an imperfection which the initial auctions and ex post exchanges of bit gold will have to address.

Epilogue

Epilogue

Thank you for reading this far.

The Popularization of Money is neither a technical white paper nor a forecast of future exchange-rate paths. After Hayek, and on the threshold of the value internet's rise, we try to answer a civilizational question: when information can travel at near-zero cost, must the transfer and bookkeeping of value still be defined by a few unauditable monopolies?

Humanity has passed through agricultural and industrial civilization and is now traversing information civilization—code, data, and networks have driven the friction of cognitive collaboration to unprecedented lows. Yet we believe society will not stop there. After information civilization comes value civilization: value units that are programmable, verifiable, and composable, so that cross-border exchange and machine-to-machine clearing need no longer depend entirely on the discretion and self-reporting of sovereign intermediaries. This is not a utopian promise, but a cautious imagination of an infrastructure in evolution.

We advance the "popularization of money" with caution: not a mania for unconstrained printing by everyone, but—under open rules—returning part of the rights to mint, hold, audit, and choose from licensed oligopolies to participants willing to bear collateral and compliance duties; letting fiat currencies with mismanaged monetary policy gradually lose space for voluntary adoption under parallel competition; and letting a fixed-supply reserve anchor and a dynamically circulating public medium each take their role in a division of labor. Every vision in this book marks the boundaries still awaiting practical test—because we know that institutional leaps without honesty collapse into narrative bubbles.

In the end, *The Popularization of Money* is essentially a large-scale social experiment. Protocols can be deployed and nodes can run, but acceptance circles, redemption channels, tax interfaces, and cross-border clearing ultimately rest on the choices of real people and institutions. It requires sovereign states to draw clear, reversible rule-spaces between tax anchors and parallel units, to allow experiment in sandboxes and mutual recognition rather than blanket bans born of fear; it requires enterprises and institutions to build on-chain treasury, supply-chain settlement, and compliance architecture as long-term capabilities, rather than treat public money as a chip for short-term arbitrage; it requires the public at large to learn, amid incomplete information, to recognize collateral, governance, and liquidity—bearing more responsibility in exchange for more participation.

This experiment has no guaranteed timetable for success, and may repeatedly stumble through crises, bans, and governance capture. Yet monetary history tells us: every major expansion of coordination tools began in hesitation and dispute at the margins, then settled into new common sense through day-after-day use. If, when you close this book, you ask with a little more precision "who issues, who verifies, who chooses," we have done our part as writers.

Whether the door to value civilization opens depends not on the release of any single version of code, but on whether we—sovereigns, entrepreneurs, developers, savers, and every person still learning—are willing to take part, with civic prudence, in this ongoing experiment.

The rules are public; the story is not yet finished. Thank you for reading this volume with us. May you, the next time you pay, mint, or refuse to accept a currency, remember that you, too, are among its authors.