Next Generation Stores of Value

Privacy, Proofs, Compute — a conditional monetary thesis

v4.1 · 605 pp · CC BY 4.0
DOI 10.5281/zenodo.18902696

The claim, in one sentence. Under sustained administrative and financial repression, a bearer asset *may* earn monetary premium if holding it preserves private settlement, portable proof, and access to verified compute after ordinary substitutes weaken — only if the service path stays stress-deliverable, demand cannot bypass the asset, self-custodied loss-bearing holders persist, and infrastructure credit stays separate.

The concession. Bitcoin's buyerless work function is the monetarily superior design; proof-of-useful-work trades monetary objectivity for capacity relevance. Nothing here supersedes Bitcoin.

Ten claims.

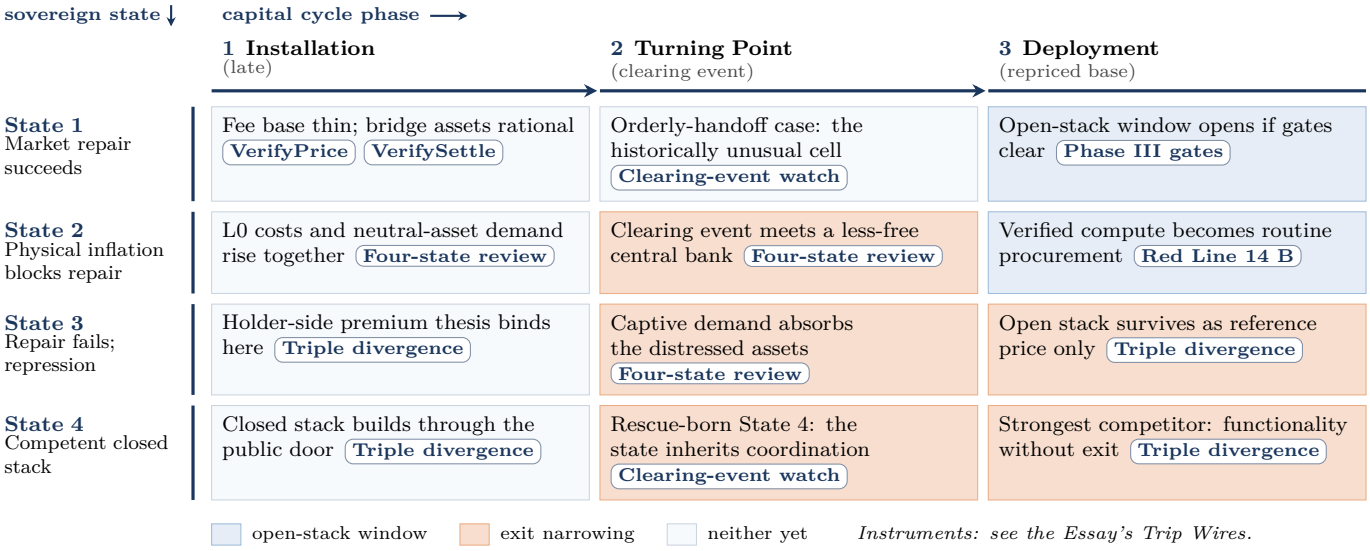
1. Fees, burns, and collateral establish accrual (a cash-flow claim and a collateral lockup), not moneyness.
2. The premium, if any, comes from three mechanisms: pledgeability without due diligence, denomination, and a state-contingent holder-side flow, which must first beat Bitcoin converted on the day.
3. Cheap public verification removes private information about *unit quality* only; fundamentals stay information-sensitive. Bitcoin is the control case.
4. The testable prediction is lower haircut *dispersion* among independently underwriting lenders, not lower levels.
5. Only succinct (M1) and probabilistic (M2) verification carry the mechanism; replication (M3) buys fault tolerance, not moneyness.
6. Gross capacity is not deliverable service: service claims are bounded by scenario max-flow through the energy-to-settlement chain.
7. The competitor is not fiat but a competent closed sovereign stack — two are under construction — which wins on capability and conditions exit.
8. Bypass is a magnitude, not a switch; the fork is the cheapest bypass and the moat is coordination, buyable by capital.
9. Price is an output to explain, never evidence to cite by itself; a separate telemetry family (VerifyFlow) reads the market machine.
10. Securities classification is examined per transaction, not per token; an ex-ante-fixed constitution narrows the exposure without clearing it.

Eighteen red lines. Named conditions, most of them read on a published series with a threshold and a clock, some only after a maturity gate; each retires or downgrades the claim at the severity its box states. Three (RL16–18) read on the monetary mechanism itself: a convenience-yield null, an information-sensitivity reversion, a denomination null.

Where it is weakest (rated by the author): six of nine chain links are *Medium* — standardized work, stress-deliverable service, market formation, non-bypassability, the holder anchor, and the premium itself, which is conditional on all of them.

What is underwritable. The verifiable stack as public infrastructure with a measurement institution attached (Kardashev Labs: observatory, receipts, one corridor, SDKs). The base-asset premium is an option to learn, not an underwriting. No token, no treasury.

Read. Sixty seconds: `https://afterfiat.xyz/start/` · Essay: `https://afterfiat.xyz/essay/` · Record: `https://afterfiat.xyz/v/4.1/read/` · The case in one sitting: `https://afterfiat.xyz/pdf/next-gen-sov-v4.1-argument.pdf` · Reviews: `https://afterfiat.xyz/reviews/`



Everything on this grid is an observable. Nothing on it is a forecast. © 2026 Jason St George, CC BY 4.0 — afterfiat.xyz

The state grid: four macro states × the capital cycle.