Adaptive PoW Monetary Policy Without Oracles: A Constructive Mechanism for Pseudo-Stability via Work-Coupled Tail Emission and Burn

Shammah Chancellor
`shammah.chancellor@proton.me`
`https://t.me/TheLotusNetwork`

February 21, 2026
Version 1.1

Abstract

This paper proposes a constructive alternative to Bitcoin that retains Proof-of-Work while enabling pseudo-stability without reliance on discretionary governance or external price oracles, offering an adversarial alternative to committee-managed indices such as CPI that depend on subjective methodology and institutional measurement. Building on the observation that PoW exposes protocol-visible security expenditure through difficulty [5] (and thus expected work per block), we specify a two-loop mechanism: (i) an adaptive, work-coupled tail emission rule defined entirely from header-observable variables and prior consensus state, and (ii) a market-driven burn mechanism (burn-to-speak [4] and partial fee burn) that provides an endogenous demand sink without any oracle. The design is expressed in expectation terms and uses homomorphic (ratio-based) update equations to avoid discontinuities and reduce manipulability. We outline a stability argument based on negative feedback between work, issuance, burn demand, and equilibrium price, and discuss implementability within Bitcoin-style daemon and validation architecture.

1 Design Goal and Constraint Set

1.1 Goal: pseudo-stability against energy

We seek pseudo-stability relative to energy (and thus, indirectly, to other comparatively stable real assets such as USD), without attempting a hard peg. The intent is practical: reduce volatility enough that fixed-cost actors (wages, supply chains, debt contracts) can use the currency without requiring constant repricing.

1.2 Constraints

- **No external oracles.** No CPI, no USD feeds, no committee-defined indices.

- **No discretionary control.** Monetary parameters should not be a strategic lever for any group.
- **PoW retained.** Difficulty/work is treated as a protocol-visible security expenditure signal.
- **Non-coercive adoption.** Demand must arise from voluntary utility and market competition.

2 Notation

Index blocks by height n.

Let:

- P_n: external price of the coin (e.g. USD/coin), treated as latent (not an oracle input).
- R_n^{boot}: bootstrap subsidy component (coins/block), predetermined, continuously decaying.
- R_n^{tail}: adaptive tail subsidy component (coins/block), protocol state variable.
- F_n: transaction fees (coins/block).
- B_n: coins burned in block n by fee-burn and burn-to-speak (coins/block).

Total coinbase subsidy is:

$$R_n := R_n^{\text{boot}} + R_n^{\text{tail}}.$$

Total net issuance in block n is:

$$\Delta S_n := R_n + F_n - B_n,$$

noting that in Bitcoin-style accounting, fees are transfers to miners unless explicitly burned.

3 Work Proxy from Header Bits: Difficulty and Expected Hashes

Let T_n be the PoW target implied by the block header field `nBits` at height n.

Define difficulty (relative to a reference target T_0):

$$D_n := \frac{T_0}{T_n}.$$

Define expected hashes per block under a uniform hash oracle:

$$\mathcal{H}_n := \frac{2^{256}}{T_n + 1},$$

(up to the standard constant-factor convention).

Both are proportional to inverse target:

$$\mathcal{H}_n \propto \frac{1}{T_n} \propto D_n.$$

We therefore define an abstract, protocol-visible work proxy W_n and allow either:

$$W_n := D_n \quad \text{or} \quad W_n := \mathcal{H}_n,$$

with the understanding that this choice affects only scaling constants, not qualitative dynamics.

4 Institutional Price Indices vs Adversarial Cost Revelation

4.1 The CPI measurement problem

Institutional price measurement systems such as the Consumer Price Index face well-documented challenges that affect their reliability for monetary policy applications. The Boskin Commission [2] identified systematic upward bias in U.S. CPI measurement, estimating annual overstatement of 1.1 percentage points due to methodological limitations including substitution bias, outlet bias, quality bias, and new product bias. Subsequent analysis by Lebow and Rudd [8] confirmed persistent measurement error despite technical improvements, noting that revision lags and subjective quality adjustments introduce uncertainty that affects real-time policy decisions.

Modern CPI construction incorporates extensive discretionary elements through hedonic quality adjustments [1], where statistical agencies make subjective determinations about the “true” price of evolving goods and services. Committee-based methodological choices—such as geometric versus arithmetic mean aggregation, seasonal adjustment parameters, and quality normalization procedures—embed institutional judgment that may not reflect market participant perceptions of purchasing power changes.

4.2 Adversarial cost revelation as alternative

PoW-based measurement offers a structural alternative based on adversarial cost revelation rather than committee consensus. Where institutional indices require subjective aggregation of basket prices and quality assessments, work-based signals derive from miners’ actual expenditure decisions under competitive pressure. The difficulty adjustment mechanism naturally incorporates changing technology costs, energy prices, and capital efficiency without requiring explicit quality adjustments or methodological committee decisions.

This adversarial approach, building on Weinstein’s framework for institutional capture resistance [13], leverages the fact that miners cannot coordinate to systematically misrepresent their cost structure without losing competitive advantage. Unlike survey-based price collection or administratively determined quality adjustments, the work proxy emerges from genuine economic competition where misrepresentation carries immediate financial consequences.

Crucially, PoW-based measurement avoids the temporal lag and revision problems that affect institutional indices. Where CPI figures undergo substantial revision as better data becomes available, blockchain difficulty adjusts automatically based on realized mining behavior, providing real-time cost signal revelation without reliance on lagged survey data or subsequent statistical correction.

4.3 Implications for monetary policy

The distinction between committee-managed and adversarially-revealed measurement becomes particularly relevant for monetary mechanisms operating without discretionary oversight. Where traditional monetary policy can adjust to CPI revision and methodological updates through central bank intervention, algorithmic systems require measurement inputs that are both timely and manipulation-resistant.

The proposed work-coupled mechanism represents an implementation of this adversarial measurement principle: rather than tracking external price indices that embed institutional methodology choices, the system responds to cost signals that emerge mechanically from competitive mining activity. This approach trades the breadth of traditional purchasing power indices for the tamper-resistance and real-time availability of adversarially-revealed work costs.

5 Mechanism Overview: Two Coupled Loops

The mechanism has two coupled components:

5.1 (A) Adaptive tail emission (source loop)

A sublinear, work-coupled tail emission adjusts the long-run issuance rate using only (W_n, W_{n-1}) and prior tail state R_n^{tail}.

5.2 (B) Market burn (sink loop)

Coins are destroyed via:

- **Partial fee burn:** a fixed fraction of transaction fees is burned.
- **Burn-to-speak:** users competitively burn coins to purchase scarce attention or posting priority, priced only in coin units (no oracle).

6 Adaptive Tail Emission Rule

6.1 Sublinear homomorphic update

Let $\gamma \in (0, 1)$ be a constant exponent; we highlight $\gamma = \frac{1}{2}$ (square-root) as a natural candidate.

Define the stateful update:

$$R_{n+1}^{\text{tail}} = \text{clip}\left(R_n^{\text{tail}} \cdot \left(\frac{W_n}{W_{n-1}} \right)^{\gamma},\ R_{\min},\ R_{\max} \right),$$

where:

- $R_{\min} > 0$ ensures persistent baseline subsidy incentive for mining.
- $R_{\max}$ prevents rare shocks or edge cases from exploding issuance.
- $\text{clip}(x, a, b) := \min(\max(x, a), b)$.

This update is *homomorphic* in the sense that it depends only on ratios of protocol-visible quantities and composes multiplicatively over time:

$$R_{n+m}^{\text{tail}} \approx R_n^{\text{tail}} \cdot \prod_{i=0}^{m-1} \left(\frac{W_{n+i}}{W_{n+i-1}} \right)^{\gamma},$$

subject to clipping.

6.2 Why sublinear ($\gamma < 1$)

If emission scaled linearly with work (effectively $\gamma = 1$), large increases in W could create runaway incentives where increased mining produces proportionally increased issuance, destabilizing equilibrium. Sublinear response ($\gamma < 1$) moderates this, preserving a negative-feedback regime.

6.3 Bootstrap component

We assume a continuously decaying bootstrap subsidy:

$$R_n^{\text{boot}} = R_0 \cdot \exp(-\lambda n),$$

chosen to attract early participation without discrete halving shocks. This component is independent of the adaptive tail and can be parameterized to distribute an initial tranche faster than Bitcoin.

6.4 Manipulation resistance of the work ratio signal

Let a miner controlling fraction μ of hashpower suppress participation by ε in block $n-1$ and restore it in block n, inflating W_n/W_{n-1}.

- Work ratio inflates to approximately $(1 - \varepsilon\mu)^{-1}$.
- Tail emission increases by $\Delta R \approx R_n^{\text{tail}} \cdot \varepsilon\mu\gamma$.
- Miner's share of gain: $\mu^2 \varepsilon\gamma R_n^{\text{tail}}$.

- Cost of suppression: $\varepsilon\mu \cdot P_n(R_n + (1-\beta)F_n)$.
- Manipulation profitable only when $\mu\gamma R_n^{\text{tail}} > P_n(R_n + (1-\beta)F_n)$.
- Since $R_n^{\text{tail}} \leq R_n$ and $\gamma < 1$, this threshold exceeds γ and approaches 1 as $\gamma \to 0$. Sublinear response therefore provides manipulation resistance that tightens as γ decreases.

7 Fixed Fee Burn and Burn-to-Speak

7.1 Fixed fee burn

Let $\beta \in (0,1)$ be a protocol constant (no oracles, no governance adjustment). For each block:

$$B_n^{\text{fee}} := \beta F_n, \qquad F_n^{\text{miner}} := (1-\beta)F_n.$$

This prevents miner self-spam "recycling" from being costless, since a fraction of fees is destroyed.

7.2 Burn-to-speak as an endogenous sink

Let $\mathcal{S}_n$ denote a set of "speech" events (posts, messages, promoted transactions) in block n, each with burn amount $b_i \geq 0$. Define:

$$B_n^{\text{b2s}} := \sum_{i \in \mathcal{S}_n} b_i, \qquad B_n := B_n^{\text{fee}} + B_n^{\text{b2s}}.$$

Attention allocation is governed by a monotone rule in b_i (e.g. rank ordering, proportional share, or auction). The burn-to-speak mechanism is formally specified as a federated anti-spam messaging protocol in [4], which provides the complete application-layer implementation including proof-of-payment construction, relay server verification, and publish-subscribe broadcasting. Importantly, b_i is chosen in coin units. External prices (USD) affect behavior only through voluntary market participation: if the coin becomes cheaper externally, advertisers can obtain and burn more coins to compete for the same attention, increasing B_n^{b2s} without any oracle. As network value scales superlinearly with user adoption [9], burn-to-speak demand may grow faster than linearly with user count, providing a natural sink that strengthens with adoption.

Demand model. Let $D(P_n)$ denote aggregate coin-denominated burn demand at external price P_n. With N advertisers each holding a fixed fiat budget b, each converts to coins and burns: $B_n^{\text{b2s}} \approx Nb/P_n$. As P_n falls, coin-denominated burn rises proportionally—the sink strengthens when price falls, which is the direction required for negative feedback. This fiat-budget mechanism makes burn demand inelastic in coin units and elastic in fiat units, providing the endogenous stabilizing response without requiring any oracle.

8 Expectation-Based Equilibrium Sketch

We reason qualitatively in expectation.

Assume (as in standard permissionless security arguments [3]) that long-run work provision is anchored to expected miner revenue in external units:

$$\mathbb{E}[W_n] \text{ increases with } \mathbb{E}[P_n] \cdot \mathbb{E}[R_n + F_n^{\text{miner}}].$$

We emphasize that P_n and k_e^* are not oracle inputs; they appear only in design-time calibration and economic interpretation.

The proposed mechanism couples:

- higher work $\Rightarrow$ higher tail emission (sublinearly),
- falling external price $\Rightarrow$ increased competitive burn-to-speak (in coin units) for a given external marketing budget,
- fee burn $\Rightarrow$ persistent sink and anti-spam cost even under miner control.

Thus net supply change in expectation is:

$$\mathbb{E}[\Delta S_n] = \mathbb{E}[R_n^{\text{boot}} + R_n^{\text{tail}} + F_n - (\beta F_n + B_n^{\text{b2s}})].$$

Pseudo-stability is sought via a negative-feedback regime where:

- rapid demand growth raises P_n and W_n,
- the tail rule increases issuance sublinearly (moderating price spikes),
- burn-to-speak and fee burn provide a sink that grows with usage/attention competition,
- the combination reduces extreme scarcity-driven volatility while preserving PoW security incentives.

No claim of perfect stability is made; the claim is that the system has an endogenous stabilizing tendency without institutional measurement. Unlike PoS systems where validators can optimize for maximal extractable value (MEV) through sophisticated infrastructure races [6, 7], PoW miners face inherently limited optimization opportunities, reducing the displacement of security expenditure into opaque channels.

8.1 Shock characterization

Shocks handled well: Gradual technology improvements (secular decline in k_e^*) and demand growth both move through the work signal, allowing the tail rule to respond proportionally.

Shocks handled poorly: Sudden energy price discontinuities shift k_e^* without an immediately visible change in W_n, creating a disequilibrium window before difficulty adjusts. Sudden large hashrate jumps (new ASIC generation) may transiently push W_n/W_{n-1} outside the stable regime; the clip bounds $(R_{\min}, R_{\max})$ contain but do not eliminate this exposure.

These limitations are inherent to oracle-free design. The relevant comparison is not to a fully-informed planner but to discretionary governance, which responds to shocks through committee decision with credibility and capture risks of its own.

Note on energy price volatility. The pseudo-stability target is stability *relative to energy cost*, not relative to fiat currency. Energy prices exhibit their own substantial volatility (e.g., natural gas prices swung approximately 5× during 2022). The coin will therefore inherit residual energy-price variance. This is a design consequence of the oracle-free constraint: energy is a real thermodynamic cost anchored in physics, unlike a committee-defined consumption basket. System designers should not expect fiat-price stability as a direct output; the intended outcome is reduction of extreme scarcity-driven volatility relative to a fixed-supply regime, not a hard peg.

8.2 Formal Stability Analysis under Linearized Dynamics

We provide a Lyapunov-based stability argument for the two-loop mechanism in a neighborhood of the equilibrium.

Setup. Define the equilibrium triple (R^*, W^*, P^*) satisfying the mining-equilibrium and supply-balance conditions:

$$P^* R^* = W^* k_e, \tag{ME}$$

$$Nb/P^* = R^*. \tag{SB}$$

Here k_e is marginal energy cost per unit work and N, b are advertiser count and fiat budget from the demand model of Section 7.2. Let log-deviations from equilibrium be:

$$r_n = \log(R_n^{\text{tail}}/R^*), \qquad w_n = \log(W_n/W^*), \qquad p_n = \log(P_n/P^*).$$

Linearized dynamics. Under three simplifying assumptions: (i) clipping is inactive near equilibrium; (ii) hashrate adjusts instantaneously to equate miner revenue with marginal cost ($W_n k_e = P_n R_n^{\text{tail}}$), giving $w_n = p_n + r_n$ to first order; and (iii) price responds to net supply deviation with sensitivity $\phi > 0$, i.e. $p_{n+1} \approx (1-\phi)p_n - \phi r_n$; substitution yields an autonomous second-order recurrence for the work deviation:

$$w_{n+1} = (1 - \phi + \gamma)\, w_n - \gamma\, w_{n-1}. \tag{1}$$

Net supply deviation satisfies $\Delta S_n/S \approx r_n + p_n = w_n$ near equilibrium, so $w_n \to 0$ implies net issuance vanishes.

Theorem 1 (Lyapunov Stability of Two-Loop Mechanism)**.** *If $\phi \in (0,\, 2 + 2\gamma)$, then the characteristic roots of recurrence* (1) *lie strictly inside the unit disk, and the following hold:*

1. *There exists a positive-definite quadratic Lyapunov function* $V_n = \mathbf{w}_n^\top P\,\mathbf{w}_n$*, where* $\mathbf{w}_n = (w_n,\, w_{n-1})^\top$*, satisfying* $\Delta V_n \le -\eta\, V_n$ *for some* $\eta > 0$*;*
2. $w_n \to 0$ *geometrically; consequently net supply deviation* $\Delta S_n/S \to 0$*;*
3. r_n *converges to a finite limit* r_∞*, and* $p_n \to -r_\infty$ *(price settles consistently with supply balance at the new level).*

Proof. The characteristic polynomial of (1) is $\chi(\lambda) = \lambda^2 - (1 - \phi + \gamma)\lambda + \gamma$, with coefficients $a_1 = -(1 - \phi + \gamma)$ and $a_0 = \gamma$. The Jury stability criterion for degree-2 discrete-time polynomials requires: (i) $|a_0| < 1$; (ii) $\chi(1) > 0$; (iii) $\chi(-1) > 0$. We verify each:

- $|a_0| = \gamma < 1$ since $\gamma \in (0, 1)$. ✓
- $\chi(1) = 1 - (1 - \phi + \gamma) + \gamma = \phi > 0$ since $\phi > 0$. ✓
- $\chi(-1) = 1 + (1 - \phi + \gamma) + \gamma = 2 + 2\gamma - \phi > 0$ iff $\phi < 2 + 2\gamma$. ✓

All conditions hold under $\phi \in (0, 2 + 2\gamma)$, so both roots satisfy $|\lambda_i| < 1$.

For any stable linear system with companion matrix A (where $A = \left(\begin{smallmatrix} 1-\phi+\gamma & -\gamma \\ 1 & 0 \end{smallmatrix}\right)$), the discrete Lyapunov equation $A^\top P A - P = -I$ admits a unique positive-definite solution P [14]. The corresponding quadratic form $V_n = \mathbf{w}_n^\top P\,\mathbf{w}_n$ satisfies $\Delta V_n = -\mathbf{w}_n^\top \mathbf{w}_n \le -\lambda_{\min}(P)^{-1} V_n$, so $\eta = \lambda_{\min}(P)^{-1} > 0$.

Geometric decay of w_n implies $\sum_n |w_n - w_{n-1}| < \infty$; since $r_{n+1} - r_n = \gamma(w_n - w_{n-1})$, the series $r_n = r_0 + \gamma \sum_{k<n}(w_k - w_{k-1})$ converges absolutely. The limit satisfies $r_\infty + p_\infty = \lim_n w_n = 0$. $\square$

Remark (Economic interpretation of stability condition). The bound $\phi < 2 + 2\gamma$ limits how aggressively price responds to supply imbalance. If price sensitivity is excessive, the combined tail-emission and price feedback overshoots, producing oscillations. The sublinear exponent γ widens the stable region: smaller γ (more conservative emission) narrows it while simultaneously improving manipulation resistance (Section 6.4). These trade-offs should inform parameter calibration.

Remark (Price-level indeterminacy). Theorem 1 guarantees convergence to *some* supply-balanced equilibrium $(R_\infty^{\text{tail}}, P_\infty)$ but not specifically to the reference pair (R^*, P^*). This reflects price-level indeterminacy standard in supply-balanced monetary models: the equilibrium *level* depends on initial conditions, while equilibrium *variance* is bounded. Anchoring to a specific price level would require an oracle or discretionary policy—excluded by design.

Scope of the argument. The formal proof applies to the linearized system near equilibrium under idealized assumptions (instantaneous hashrate adjustment, clipping inactive, fiat-budget burn demand). Nonlinear effects, discrete halving shocks, and clip-bound saturation are outside the scope of this argument; their effects are addressed via simulation in Section 12.

9 Implementation Notes (Bitcoin-style daemon)

9.1 No coinbase lookups required

R_n^{tail} is defined as *subsidy only* (excludes fees). Nodes maintain R_n^{tail} as a consensus state variable in chainstate/index, computed deterministically from:

$$(R_{n-1}^{\text{tail}}, W_{n-1}, W_{n-2}).$$

During validation, enforce:

$$\text{coinbase subsidy} \leq R_n^{\text{boot}} + R_n^{\text{tail}},$$

while fees are handled as usual (with fixed burn fraction applied by consensus rules).

9.2 Header-only work proxy

W_n is derived directly from `nBits` (target bits), so only recent headers are needed. No full-history scan is required.

9.3 Fixed-point arithmetic

To avoid floating-point nondeterminism, implement $(W_n/W_{n-1})^\gamma$ using fixed-point rational approximation; for $\gamma = \frac{1}{2}$, integer square-root methods are simple and stable.

10 Discussion: Adoption and Non-Coercive Bootstrapping

The design is non-coercive: demand arises from voluntary utility. Burn-to-speak requires an attention surface; thus, a practical bootstrapping pathway is to deploy the system within a domain where attention is already scarce (community, publishing, spam-prone forums) so that burning has immediate utility. CashWeb [4] provides exactly such an application layer: a federated messaging protocol in which the burn-to-speak mechanism functions simultaneously as spam deterrence at the application level and as an endogenous supply sink at the monetary level. Deployment within the CashWeb messaging network therefore bootstraps both utility and monetary stability in a single system. The accelerated bootstrap tranche can attract early participation, while long-run dynamics are governed by the tail+burn loops rather than perpetual scarcity shocks.

Cold-start regime. The stability guarantees of Theorem 1 assume nonzero burn demand; they do not apply in the cold-start regime where burn-to-speak activity is negligible. During this phase the sink loop is effectively inactive and issuance is governed by R_n^{boot} alone. Cold-start is not a failure mode but a known design phase: the bootstrap component is sized precisely to sustain mining participation while the application-layer network effect accumulates. The stability guarantees become operative once burn demand is large enough that B_n^{b2s} meaningfully offsets issuance—a threshold that should be estimated during parameter calibration based on projected early-adopter counts.

11 Parameter Derivation and Calibration (Deferred Numerical Choice)

This section derives how key parameters may be chosen from a reference equilibrium. Numerical values are intentionally deferred to implementation, since they depend on hardware efficiency, prevailing electricity prices, desired baseline security, and the intended "mature" operating regime.

11.1 Reference equilibrium

Fix a target external price level P^* (e.g. $P^* = \$0.01$ per coin, i.e. 100 coins per USD) and a reference operating point characterized by:

- W^*: a reference work proxy per block (derived from header difficulty/target),
- k_e^*: marginal external cost per unit work (USD per W-unit), interpreted as electricity+hardware OPEX on the marginal miner,
- F^*: reference fee volume in coins per block,
- β: fixed fee-burn fraction (protocol constant).

Let the miner-received fee component be $(1-\beta)F^*$, and let total subsidy be

$$R^* = R^{\text{boot},*} + R^{\text{tail},*}.$$

A first-order equilibrium condition equates expected external miner revenue per block to marginal external cost:

$$P^*\big(R^* + (1-\beta)F^*\big) \approx W^* k_e^*.$$

Solving for the required total subsidy gives:

$$R^* \approx \frac{W^* k_e^*}{P^*} - (1-\beta)F^*.$$

Given a chosen bootstrap schedule value $R^{\text{boot},*}$ at that epoch, the implied tail level is:

$$R^{\text{tail},*} \approx R^* - R^{\text{boot},*}.$$

11.2 Initializing and bounding the tail state

The stateful tail rule

$$R^{\text{tail}}_{n+1} = \text{clip}\left(R^{\text{tail}}_n \cdot \left(\frac{W_n}{W_{n-1}}\right)^{\gamma},\ R_{\min},\ R_{\max}\right)$$

does not require a separate scaling constant. Instead, one chooses:

- an initial state R_0^{tail} (e.g. set near $R^{\text{tail},*}$ for the intended launch regime),
- a positive floor $R_{\min} > 0$ to preserve baseline mining incentive under demand collapse,
- optionally a cap $R_{\max}$ as a safety invariant against rare shocks or corner cases.

In practice, $R_{\min}$ may be specified as a fraction of the reference tail level, $R_{\min} = \eta R^{\text{tail},*}$ for some $\eta \in (0, 1)$, while $R_{\max}$ may be set "sufficiently large" or treated as an explicit invariant. All such numerical choices are deferred to implementation and empirical testing.

11.3 Choosing the sublinearity exponent

The exponent $\gamma \in (0, 1)$ governs responsiveness and avoids linear-in-work runaway incentives. A natural candidate is $\gamma = \frac{1}{2}$ (square-root), but the protocol may treat γ as a fixed constant selected during implementation after simulation and adversarial analysis.

11.4 Interpretation

The calibration equations above provide a bridge between (i) a desired external price regime P^* and (ii) an intended baseline security/work regime W^* given external energy/hardware costs. The protocol itself does not observe P^* or k_e^*; these are design-time calibration quantities used only to select initial constants.

12 Simulation and Validation Checklist

Prior to deployment, the following simulations are sufficient to validate qualitative behavior and bound parameter choices. No external oracles are required.

- **Parameter sweeps:** Vary $\gamma \in (0, 1)$ (with emphasis on $\gamma = \frac{1}{2}$), fee burn fraction β, tail floor $R_{\min}$, and initial tail state R_0^{tail}.
- **Demand shocks:** Introduce step and impulse shocks to transaction demand and burn-to-speak activity; observe convergence of R_n^{tail} and net issuance ΔS_n.
- **Mining shocks:** Simulate sudden increases/decreases in available hashpower (e.g. ASIC generation changes) and verify bounded issuance response under the sublinear rule.
- **Adversarial scenarios:** Model miner self-spam attempts, fee recycling, and temporary mining griefing to confirm fixed fee burn imposes irreducible cost.
- **Long-run saturation:** Hold user/activity proxies constant and verify that issuance converges to a steady regime rather than linear growth.

- **Numerical stability:** Validate fixed-point arithmetic bounds and clipping invariants to ensure deterministic behavior across implementations.

These simulations are intended to validate stability and incentive structure rather than to predict exact price trajectories.

13 Conclusion

We specified a PoW-based monetary mechanism that (i) uses only protocol-visible work signals for adaptive tail emission and (ii) incorporates an oracle-free burn sink via fee burn and burn-to-speak. The resulting system aims for pseudo-stability against energy by coupling issuance and burn to adversarially revealed work and endogenous attention competition, avoiding discretionary issuance and institutional measurement. This approach demonstrates how adversarial cost revelation can substitute for committee-managed price indices in algorithmic monetary policy design. Further work should formalize stability conditions under explicit behavioral assumptions and explore parameter regimes for γ, $(R_{\min}, R_{\max})$, and β.

References

[1] Bureau of Labor Statistics. Hedonic Quality Adjustment in the CPI. U.S. Department of Labor, 2019. `https://www.bls.gov/cpi/quality-adjustment/hedonic-quality-adjustment.htm`

[2] M. J. Boskin, E. R. Dulberger, R. J. Gordon, Z. Griliches, and D. W. Jorgenson. Toward a More Accurate Measure of the Cost of Living: Final Report to the Senate Finance Committee from the Advisory Commission to Study the Consumer Price Index. U.S. Senate Finance Committee, 1996. `https://www.ssa.gov/history/reports/boskinrpt.html`

[3] E. Budish. The Economic Limits of Bitcoin and the Blockchain. *Journal of Political Economy*, 130(3):636–678, 2022.

[4] S. Chancellor. CashWeb: A Cryptocurrency-Integrated Protocol for Federated Anti-Spam Messaging and Publish-Subscribe Systems. Preprint, 2026.

[5] S. Chancellor. Security Expenditure, Energy, and Issuance Legibility in Permissionless Consensus. Preprint, 2026.

[6] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *2020 IEEE Symposium on Security and Privacy*, pages 910–927, 2020.

[7] Flashbots Research. MEV-Explore: A Live Dashboard of MEV Activity. `https://explore.flashbots.net/`, 2021.

[8] D. E. Lebow and J. B. Rudd. Measurement error in the Consumer Price Index: where do we stand? *Journal of Economic Literature*, 41(1):159–201, 2003.

[9] B. Metcalfe. Metcalfe's Law: A Network Becomes More Valuable as It Reaches More Users. *Infoworld*, 17(40):53–54, 1995.

[10] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. `https://bitcoin.org/bitcoin.pdf`

[11] N. Plassaras. Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law*, 14(1):377–407, 2013.

[12] P. Todd. Surprisingly, tail emission is not inflationary. 2022. `https://petertodd.org/2022/surprisingly-tail-emission-is-not-inflationary`

[13] E. Weinstein. Adversarial Measurement and the Information Economy. The Portal with Eric Weinstein, 2021.

[14] H. K. Khalil. *Nonlinear Systems*, third edition. Prentice Hall, 2002. (Discrete-time Lyapunov theory: Theorem 4.7 and surrounding material.)