Security Expenditure, Energy, and Issuance Legibility in Permissionless Consensus

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

February 21, 2026
Version 1.1

Abstract

Proof-of-Stake (PoS) systems are commonly described as environmentally efficient alternatives to Proof-of-Work (PoW) on the basis that they avoid continuous hashing. This paper analyzes consensus security from an equilibrium, expectation-based perspective and shows that for any permissionless system offering an externally valued block reward, rational attackers and defenders are incentivized to expend real resources proportional to the expected value at risk. Proof-of-Work expresses this expenditure directly and legibly via energy consumption, while Proof-of-Stake displaces it into heterogeneous and opaque channels such as infrastructure duplication, validator identity proliferation, MEV-driven optimization, governance capture, and institutional overhead. We further show that PoW uniquely provides a protocol-visible measure of security expenditure per unit of issuance, enabling algorithmic reasoning about monetary policy without reliance on social or institutional oracles. These results undermine the claim that PoS eliminates energy costs in equilibrium and establish PoW as a distinct ontological substrate for legible, adversarially revealed security.

1 Introduction

Environmental critiques of Proof-of-Work have driven widespread adoption of Proof-of-Stake consensus mechanisms. The dominant narrative asserts that PoS achieves comparable security with substantially lower energy consumption, since validators need only perform lightweight computation.

This paper argues that such comparisons rest on a category error. In any permissionless consensus system offering an externally priced block reward, equilibrium security expenditure is anchored to the expected value of that reward. Rational adversaries will expend resources up to the expected gain from attack, and rational defenders must expend comparable resources to deter capture. This is a direct application of competitive rent dissipation [1, 2], most recently applied to blockchain

consensus by Budish [3]. Changing the consensus mechanism alters the *form* and *visibility* of expenditure, but not its existence.

We show that Proof-of-Work uniquely renders security expenditure legible to the protocol itself, while Proof-of-Stake displaces equivalent expenditure into less measurable and often less efficient institutional forms. This distinction has implications not only for energy accounting, but for monetary design.

2 Block Rewards and Equilibrium Security Expenditure

Let time be indexed by block height t. Define:

- P_t: external price of the native asset (e.g. USD/coin),
- R_t: issuance (coins/block),
- F_t: transaction fees (coins/block),
- M_t: additional extractable value (coins/block).

Define the total block reward in coins:

$$\Pi_t := R_t + F_t + M_t,$$

and its external value:

$$V_t := P_t \cdot \Pi_t.$$

All quantities are potentially stochastic; we therefore reason in expectation.

2.1 Attack incentives

An attacker is incentivized to attack whenever:

$$\mathbb{E}[G_t] - \mathbb{E}[C_t^{\text{att}}] > 0,$$

where G_t is the external gain from the attack and C_t^{att} is the external cost incurred.

In open-entry, competitive environments, persistent opportunities to capture V_t at cost far below V_t are eliminated. Consequently, equilibrium attacker expenditure satisfies:

$$\mathbb{E}[C_t^{\text{att}}] \approx \alpha\, \mathbb{E}[V_t],$$

for some $\alpha \in (0, 1]$, with $\alpha > 1$ possible when attacks unlock additional external payoffs.

2.2 Defense incentives

To deter attack, defenders must raise attacker costs or match attacker capability. In either case:

$$\mathbb{E}[C_t^{\text{def}}] \gtrsim \mathbb{E}[C_t^{\text{att}}] \approx \alpha\, \mathbb{E}[V_t].$$

Thus equilibrium security expenditure is lower-bounded by expected value at risk, independent of consensus mechanism.

3 External Cost as a Security Axiom

The original Bitcoin whitepaper implicitly relies on the principle that durable security requires irrecoverable external expenditure [4]. We elevate this assumption to an explicit axiom.

Axiom (External Cost of Control). *In a permissionless consensus system, durable control over state transitions requires irreversible expenditure in a substrate priced external to the system itself.*

This axiom does not specify the substrate, only that it be external, costly, and non-recoverable.

4 Embodiment Principle

Principle (Substrate Embodiment). *Any strategic expenditure in a real-world game must be instantiated in an ontological substrate, and therefore entails non-zero resource and energy consumption specific to that substrate.*

Expenditures on hardware, labor, buildings, coordination, governance, and enforcement all entail embodied energy through production and operation. Energy use may be direct or indirect, but cannot be eliminated if external cost is required.

This principle establishes that PoS security expenditure is nonzero but does not by itself establish the magnitude. The relevant comparison is not existence but scale: does displaced PoS expenditure approach PoW expenditure for equivalent security levels? This depends on which channels absorb the displaced expenditure and their energy intensity relative to direct hashing. Section 6 develops the claim that the relevant channels—MEV infrastructure, validator redundancy, governance coordination—are energetically embodied at scales comparable to direct mining expenditure for equivalent security levels.

5 Proof-of-Work and Legible Security Expenditure

In Proof-of-Work systems, security expenditure is expressed directly through energy consumption.

Let:

- $\mathcal{H}_t$: expected hashes required per block (a function of difficulty),

- e_t: joules per hash,
- c_t: price of electricity (USD/joule).

Expected electricity cost per block is:

$$\mathbb{E}[C_t^{\text{pow}}] = \mathbb{E}[\mathcal{H}_t\, e_t\, c_t] + \mathbb{E}[\text{overhead}_t].$$

For an attack requiring control for k blocks, deterrence requires:

$$\mathbb{E}[\mathcal{H}_{t,k}^{\text{att}}\, e_t\, c_t] \gtrsim \mathbb{E}[k\, P_t \Pi_t].$$

Rearranging yields an implied price bound:

$$\mathbb{E}[P_t] \lesssim \frac{\mathbb{E}[\mathcal{H}_{t,k}^{\text{att}}\, e_t\, c_t]}{\mathbb{E}[k\, \Pi_t]}.$$

5.1 Protocol-visible security density

Crucially, PoW protocols observe $\mathcal{H}_t$ and Π_t directly. The daemon can therefore compute:

$$\sigma_t := \frac{\mathcal{H}_t}{\Pi_t},$$

the expected irreversible work backing each unit of issuance.

This provides a live, adversarially revealed, protocol-native measure of security expenditure per coin. No equivalent quantity exists in Proof-of-Stake systems.

The game-theoretic properties of σ_t as a signal deserve attention. Two questions arise. First, is σ_t manipulable by large miners? Since $\mathcal{H}_t$ is determined by difficulty (a lagged average over many blocks), short-run manipulation has limited effect; sustained misrepresentation requires foregoing block rewards at a rate that exceeds the manipulation gain for any $\mu < 1/2$. Second, what are the equilibrium dynamics if monetary policy responds to σ_t? If issuance adjusts in response to σ_t, miners anticipate this and adjust hashrate accordingly—a strategic response that the adaptive monetary mechanism must account for. These dynamics are analyzed in [5].

Remark (Lagged Signal). Because difficulty is computed as a rolling average over many blocks (2016 blocks in Bitcoin), σ_t reflects historical rather than instantaneous security expenditure. A rapid collapse in hashpower—for example, a regulatory shutdown of a dominant mining region—leaves σ_t artificially elevated for up to the full difficulty adjustment window before the difficulty algorithm corrects. Systems that use σ_t as an adaptive signal must account for this lag, either through conservative response parameters or by monitoring auxiliary real-time signals such as observed block interval variance.

6 Displaced Expenditure in Proof-of-Stake

Proof-of-Stake eliminates continuous hashing but does not eliminate the incentive to expend resources up to $\mathbb{E}[V_t]$. Instead, expenditure is displaced into multiple channels:

- validator identity proliferation and infrastructure duplication,
- MEV-driven optimization, latency races, and specialized hardware,
- governance capture, coordination, and enforcement,
- custodial, legal, and compliance overhead.

Let C_t^{pos} denote total external cost across all such channels. Equilibrium security requires:

$$\mathbb{E}[C_t^{\text{pos}}] \gtrsim \alpha\, \mathbb{E}[V_t].$$

These costs remain energetically embodied but are not protocol-legible and are difficult to audit or optimize.

Remark (Threat Model Asymmetry). The expenditure comparison above assumes attacks directed at the same objective: controlling a sufficient fraction of active consensus participation to rewrite recent history. However, PoW and PoS face categorically different attack vectors. PoS systems are additionally vulnerable to *long-range attacks*: an adversary who acquires old validator private keys (from early participants, compromised exchanges, or slashable deposits that have since been withdrawn) can potentially rewrite history from an earlier epoch at negligible cost, since those keys carry no ongoing economic exposure. This attack is prohibitively expensive in PoW—rewriting blocks requires re-expending the energy for every block in the rewritten chain, an irreducibly physical constraint. The rent-dissipation framework characterizes equilibrium expenditure for ongoing participation; it does not capture the asymmetric cost of this qualitatively distinct attack class. PoS systems address this through weak subjectivity checkpoints or social consensus on finality, reintroducing institutional coordination that the rent-dissipation model did not require.

7 Issuance, Throughput, and Misattributed Constraints

A common misconception is that Proof-of-Work inherently limits transaction throughput. This conflates consensus with capacity planning. PoW determines leader selection and security cost; throughput is determined by block size, block frequency, and network design.

Observed throughput limitations in Bitcoin arise from explicit parameter choices and governance decisions, not from Proof-of-Work itself.

8 Human-Controlled Issuance and Strategic Failure

Any issuance mechanism dependent on human discretion introduces repeated-game incentives, asymmetric information, and strategic capture. Over time, such systems exhibit credibility erosion and over-issuance.

By contrast, PoW exposes an adversarially generated, non-social signal of security expenditure. Issuance mechanisms that respond algorithmically to this signal avoid discretionary control and institutional oracles.

9 Conclusion

We have shown that equilibrium security expenditure in permissionless consensus is anchored to expected external value at risk. Proof-of-Work expresses this expenditure directly and legibly through energy consumption and uniquely provides a protocol-visible measure of security expenditure per unit of issuance. Proof-of-Stake does not eliminate energy costs in equilibrium; it displaces them into opaque and often less efficient institutional forms.

These results undermine claims that PoS is inherently environmentally superior and establish PoW as a distinct ontological substrate for legible, adversarially revealed security. The implications for monetary design and adaptive issuance are developed in [5], which specifies an oracle-free two-loop mechanism using the work proxy σ_t as an adaptive issuance signal. The protocol-level instantiation of burn-to-speak as an anti-spam federated messaging layer is specified in [6].

References

[1] G. Tullock. Efficient rent seeking. In J. Buchanan, R. Tollison, and G. Tullock, editors, *Toward a Theory of the Rent-Seeking Society*, pages 97–112. Texas A&M University Press, 1980.

[2] A. O. Krueger. The political economy of the rent-seeking society. *American Economic Review*, 64(3):291–303, 1974.

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

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

[5] S. Chancellor. Adaptive PoW Monetary Policy Without Oracles: A Constructive Mechanism for Pseudo-Stability via Work-Coupled Tail Emission and Burn. Preprint, 2026.

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