无许可共识中的安全支出、能源与发行量可读性

Shammah Chancellor

shammah.chancellor@proton.me

https://t.me/TheLotusNetwork

2026 年 2 月 21 日

Version 1.1

摘要

权益证明（PoS）系统通常被描述为工作量证明（PoW）的环保替代方案，理由是其避免了持续哈希运算。本文从均衡、期望视角分析共识安全性，证明对于任何提供具有外部价值的区块奖励的无许可系统，理性的攻击者和防御者都受到激励，按与风险敞口的预期价值成比例地消耗实际资源。工作量证明通过能源消耗直接且清晰地表达这种支出；而权益证明则将其转移至多样化且不透明的渠道，例如基础设施冗余、验证者身份增殖、MEV 驱动的优化、治理捕获以及机构运营开销。我们进一步证明，PoW 独特地提供了一种协议可见的每单位发行量安全支出度量，使货币政策的算法推理无需依赖社会性或机构性预言机。上述结论动摇了"PoS 在均衡状态下消除能源成本" 的论断，并确立了 PoW 作为可读、对抗性揭示安全性的独特本体论基底的地位。

1 引言

对工作量证明的环境批评推动了权益证明共识机制的广泛采用。主流叙事断言，PoS 以显著更低的能源消耗实现了与 PoW 相当的安全性，因为验证者仅需执行轻量级计算。

本文认为，此类比较建立在一个范畴性错误之上。在任何提供外部定价区块奖励的无许可共识系统中，均衡安全支出与该奖励的预期价值相锚定。理性攻击者将消耗资源直至预期攻击收益，理性防御者则必须消耗相当资源以阻止捕获。这是竞争性租金耗散的直接应用 [1, 2]，最近由 Budish 将其应用于区块链共识 [3]。改变共识机制只能改变支出的*形式*与*可见性*，而非其存在本身。

我们证明，工作量证明独特地使安全支出对协议本身保持可读，而权益证明则将等量支出转移至可测量性较低、通常效率也较低的机构形式中。这一区别不仅对能源核算具有影响，对货币设计亦然。

2 区块奖励与均衡安全支出

设时间以区块高度 t 为索引。定义：

- P_t：原生资产的外部价格（例如，美元/枚），
- R_t：发行量（枚/区块），
- F_t：交易手续费（枚/区块），
- M_t：额外可提取价值（枚/区块）。

定义以币计的总区块奖励：

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

及其外部价值：

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

所有量均可能具有随机性；因此我们在期望意义下进行推理。

2.1 攻击激励

当且仅当以下条件成立时，攻击者具有发动攻击的激励：

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

其中 G_t 为攻击所获外部收益，C_t^{att} 为所承担的外部成本。

在开放准入、充分竞争的环境中，以远低于 V_t 的代价持续捕获 V_t 的机会将被消除。因此，均衡状态下攻击者支出满足：

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

其中 $\alpha \in (0, 1]$；当攻击可解锁额外外部收益时，$\alpha > 1$ 亦属可能。

2.2 防御激励

为阻止攻击，防御者必须提高攻击者成本或匹配攻击者能力。在任一情形下：

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

因此，均衡安全支出的下界由风险敞口的预期价值决定，与共识机制无关。

3 外部成本作为安全公理

比特币白皮书原文隐含地依赖一个原理：持久安全需要不可恢复的外部支出 [4]。我们将该假设提升为明确的公理。

公理（控制的外部成本，外部成本公理）。 *在无许可共识系统中，对状态转换的持久控制需要在系统外部定价的基底中进行不可逆支出。*

该公理不规定基底的具体形式，仅要求其为外部的、有成本的且不可恢复的。

4 实体化原理

原理（基底实体化，实体化原理）。 *现实世界博弈中的任何战略性支出必须在某一本体论基底中实例化，因而必然产生该基底特有的非零资源与能源消耗。*

对硬件、劳动力、建筑物、协调机制、治理及执行的支出，均通过生产与运营过程蕴含具身能源。能源使用可以是直接的或间接的，但若要求外部成本，则无法消除。

该原理确立了 PoS 安全支出非零这一事实，但本身并不确定其量级。相关比较并非关乎是否存在，而是关乎规模：对于等效安全级别，被转移的 PoS 支出是否接近 PoW 支出？这取决于哪些渠道吸收了被转移的支出，以及相对于直接哈希运算，这些渠道的能源强度如何。第 6节将论述：相关渠道——MEV 基础设施、验证者冗余、治理协调——在等效安全级别下，其能源具身规模与直接挖矿支出相当。

5 工作量证明与可读的安全支出

在工作量证明系统中，安全支出通过能源消耗直接表达。

设：

- $\mathcal{H}_t$：每区块所需的预期哈希次数（难度的函数），
- e_t：每次哈希消耗的焦耳数，
- c_t：电价（美元/焦耳）。

每区块预期电力成本为：

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

对于需要控制 k 个区块的攻击，威慑要求：

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

整理后得到隐含价格上界：

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

5.1 协议可见的安全密度

关键在于，PoW 协议直接观测 $\mathcal{H}_t$ 与 Π_t。因此，守护进程可以计算：

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

即支撑每单位发行量的预期不可逆工作量。

这提供了一个实时的、对抗性揭示的、协议原生的每枚币安全支出度量。权益证明系统中不存在等价量。

σ_t 作为信号的博弈论性质值得关注。这里有两个问题需要探讨。第一，σ_t 是否可被大型矿工操纵？由于 $\mathcal{H}_t$ 由难度决定（难度是多个区块上的滞后平均值），短期操纵效果有限；持续的虚假呈现要求以超过操纵收益的速率放弃区块奖励，对任何 $\mu < 1/2$ 的情形均如此。第二，若货币政策响应 σ_t，均衡动态如何？若发行量根据 σ_t 进行调整，矿工会预期这一点并相应调整算力——这是自适应货币机制必须考虑的战略响应。这些动态在 [5] 中进行了分析。

注记（滞后信号）。由于难度是多个区块上的滚动平均值（比特币为 2016 个区块），σ_t 反映的是历史的而非瞬时的安全支出。算力的急剧下降——例如主要矿区遭监管关停——会使 σ_t 在整个难度调整窗口期内保持人为偏高。将 σ_t 用作自适应信号的系统必须考虑这一滞后，可通过保守响应参数或实时监控辅助信号（如观测到的出块间隔方差）加以缓解。

6 权益证明中的支出转移

权益证明消除了持续哈希运算，但并未消除将资源支出至 $\mathbb{E}[V_t]$ 的激励。取而代之，支出被转移至多个渠道：

- 验证者身份增殖与基础设施冗余，
- MEV 驱动的优化、延迟竞争与专用硬件，
- 治理捕获、协调与执行，
- 托管、法律与合规运营开销。

设 C_t^{pos} 表示所有上述渠道的总外部成本。均衡安全要求：

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

这些成本仍具有能源具身性，但不具备协议可读性，且难以审计或优化。

注记（威胁模型的不对称性）。上述支出比较假设攻击针对相同目标：控制足够份额的活跃共识参与以改写近期历史。然而，PoW 与 PoS 面临在类别上截然不同的攻击向量。PoS 系统额外面临*长程攻击*风险：攻击者获取旧验证者私钥（来自早期参与者、交易所或已提取的可罚没押金），可以极低成本从早期时期改写历史，因为这些密钥已无持续经济敞口。而在 PoW 中，此类攻击的成本极为高昂——改写区块链需要重新消耗被改写链段内每个区块所需的能量，这是不可约的物理约束。租金耗散框架刻画的是持续参与成本的均衡支出；它未能充分捕捉这一类别上不同的攻击的成本，后者需要通过主观弱确定性检查点或社会共识等独立机制加以应对。

7 发行量、吞吐量与错误归因的约束

一个常见误解是，工作量证明本质上限制了交易吞吐量。这混淆了共识与容量规划。PoW 决定领导者选举与安全成本；吞吐量由区块大小、出块频率及网络设计决定。

比特币中观测到的吞吐量限制源于明确的参数选择与治理决策，而非工作量证明本身。

8 人为控制的发行量与战略失败

任何依赖人为裁量的发行量机制都会引入重复博弈激励、信息不对称和战略捕获。随着时间推移，此类系统表现出公信力侵蚀和过度发行。

相比之下，PoW 暴露出一个对抗性生成的、非社会性的安全支出信号。以算法方式响应这一信号的发行量机制可以避免裁量控制和机构性预言机。

9 结论

我们已证明，无许可共识中的均衡安全支出与风险敞口的预期外部价值相锚定。工作量证明通过能源消耗直接且清晰地表达这一支出，并独特地提供了一种协议可见的每单位发行量安全支出度量。权益证明在均衡状态下并未消除能源成本；它只是将其转移至不透明且通常效率更低的机构形式中。

上述结论动摇了"PoS 在环境上本质上更优" 的论断，并确立了 PoW 作为可读、对抗性揭示安全性的独特本体论基底的地位。货币设计与自适应发行量方面的含义在 [5] 中进一步展开，该文献

规定了一种使用工作代理量 σ_t 作为自适应发行量信号的无预言机双环机制。将燃烧发言（burn-to-speak）作为抗垃圾消息联邦消息层的协议级实例化在 [6] 中详细说明。

参考文献

[1] G. Tullock. Efficient rent seeking. In J. Buchanan, R. Tollison, and G. Tullock, editors, 寻租社会理论探析, pages 97–112. 德克萨斯农工大学出版社, 1980.

[2] A. O. Krueger. The political economy of the rent-seeking society. 美国经济评论, 64(3):291–303, 1974.

[3] E. Budish. The economic limits of Bitcoin and the blockchain. 政治经济学杂志, 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. 预印本, 2026.

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