无预言机的自适应工作量证明货币政策：基于工作耦合尾部发行与销毁的伪稳定性构造机制

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

2026 年 2 月 21 日
Version 1.1

摘要

本文提出一种保留工作量证明（PoW）的比特币构造性替代方案，在不依赖自由裁量治理或外部价格预言机的前提下实现伪稳定性，并提供一种对抗性替代方案，以取代依赖主观方法论和机构测量的委员会管理指数（如消费者价格指数）。基于 PoW 通过难度向协议暴露安全支出这一观察 [5]（从而暴露每区块的预期工作量），本文规定了一种双环机制：(i) 一种自适应的工作耦合尾部发行规则，完全由区块头可观测变量与先前共识状态定义；(ii) 一种市场驱动的销毁机制（燃烧发言，burn-to-speak [4]，以及部分手续费销毁），在无需任何预言机的情况下提供内生需求汇。该设计以期望值形式表达，并采用同态（基于比率）的更新方程，以避免不连续性并降低可操纵性。本文概述了一种基于工作量、发行量、销毁需求与均衡价格之间负反馈的稳定性论证，并讨论了在比特币风格守护进程与验证架构中的可实现性。

1 设计目标与约束集

1.1 目标：相对能源的伪稳定性

我们寻求相对于能源（以及由此间接相对于其他较为稳定的实物资产，如美元）的伪稳定性，而不是追求硬钉住汇率。其意图是务实的：将波动性降低到足以让固定成本参与者（工资、供应链、债务合同）在无需持续重定价的情况下使用该货币。

1.2 约束条件

- **无外部预言机。**不使用消费者价格指数、美元汇率喂价，也不使用委员会定义的指数。
- **无自由裁量控制。**货币参数不应成为任何群体的战略杠杆。
- **保留工作量证明。**难度/工作量被视为协议可见的安全支出信号。
- **非强制性采用。**需求必须来源于自愿效用与市场竞争。

2 符号说明

以高度 n 对区块进行索引。
定义：

- P_n：币的外部价格（例如美元/币），视为潜在变量（非预言机输入）。
- R_n^{boot}：启动期补贴分量（币/区块），预先确定，持续衰减。
- R_n^{tail}：自适应尾部补贴分量（币/区块），协议状态变量。
- F_n：交易费（币/区块）。
- B_n：第 n 个区块中通过手续费销毁与燃烧发言销毁的币数（币/区块）。

铸币区块总补贴为：

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

第 n 个区块的总净发行量为：

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

注意，在比特币风格的记账中，手续费是转移给矿工的，除非被明确销毁。

3 从区块头位字段得到的工作代理：难度与预期哈希数

令 T_n 为高度 n 处区块头字段 `nBits` 所隐含的工作量证明目标值。
定义难度（相对于参考目标 T_0）：

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

定义在均匀哈希预言机下每区块的预期哈希数：

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

（遵循标准常数因子约定）。
两者均与目标值的倒数成比例：

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

因此，我们定义一个抽象的、协议可见的工作代理 W_n，并允许以下两种形式之一：

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

其中的理解是，这一选择仅影响缩放常数，而非定性动态。

4 机构价格指数与对抗性成本揭示

4.1 消费者价格指数的测量问题

消费者价格指数等机构价格测量体系面临有据可查的挑战，这些挑战影响其在货币政策应用中的可靠性。博斯金委员会 [2] 发现美国消费者价格指数测量存在系统性高估偏差，估计由于替代偏差、销售渠道偏差、质量偏差和新产品偏差等方法论局限，每年高估约 1.1 个百分点。Lebow 与 Rudd [8] 的后续分析证实，尽管技术有所改进，测量误差依然持续存在，并指出修订滞后和主观质量调整引入的不确定性会影响实时政策决策。

现代消费者价格指数的构建通过享乐质量调整 [1] 纳入了大量自由裁量要素，统计机构对不断演变的商品和服务的" 真实" 价格作出主观判断。基于委员会的方法论选择——例如几何均值与算术均值聚合、季节调整参数以及质量标准化程序——内嵌了机构判断，而这种判断未必反映市场参与者对购买力变化的感知。

4.2 对抗性成本揭示作为替代方案

基于工作量证明的测量提供了一种基于对抗性成本揭示而非委员会共识的结构性替代方案。机构指数需要对一篮子商品价格和质量评估进行主观聚合，而基于工作量的信号则来源于矿工在竞争压力下的实际支出决策。难度调整机制自然地将技术成本变化、能源价格和资本效率纳入考量，无需明确的质量调整或方法论委员会决策。

这种对抗性方法建立在 Weinstein 抵抗机构俘获框架 [13] 的基础上，利用了以下事实：矿工无法在不损失竞争优势的情况下协调系统性地虚报其成本结构。与基于调查的价格采集或行政确定的质量调整不同，工作代理产生于真实的经济竞争，其中虚报行为会立即带来财务后果。

至关重要的是，基于工作量证明的测量避免了影响机构指数的时间滞后和修订问题。机构消费者价格指数数据会随着更好数据的获取而进行大幅修订，而区块链难度则会根据已实现的挖矿行为自动调整，提供实时成本信号揭示，无需依赖滞后的调查数据或后续统计修正。

4.3 对货币政策的启示

在不受自由裁量监督的货币机制中，委员会管理测量与对抗性揭示测量之间的区别尤为重要。传统货币政策可以通过央行干预来适应消费者价格指数的修订和方法论更新，而算法系统则需要既及时又抗操纵的测量输入。

所提出的工作耦合机制是这一对抗性测量原则的一种实现：系统响应的是从竞争性挖矿活动中机械涌现的成本信号，而非追踪内嵌机构方法论选择的外部价格指数。这种方法以传统购买力指数的广度为代价，换取对抗性揭示的工作成本的抗篡改性和实时可用性。

5 机制概述：两个耦合环路

该机制包含两个耦合组件：

5.1 （A）自适应尾部发行（源环路）

一种次线性的工作耦合尾部发行，仅使用 (W_n, W_{n-1}) 和先前尾部状态 R_n^{tail} 来调整长期发行率。

5.2 （B）市场销毁（汇环路）

通过以下方式销毁币：

- **部分手续费销毁**：固定比例的交易费被销毁。
- **燃烧发言**：用户竞争性地销毁币以购买稀缺的注意力或发帖优先级，仅以币为单位定价（无预言机）。

6 自适应尾部发行规则

6.1 次线性同态更新

令 $\gamma \in (0,1)$ 为常数指数；我们着重强调 $\gamma = \frac{1}{2}$（平方根）作为自然候选值。
定义有状态更新：

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

其中：

- $R_{\min} > 0$ 确保对挖矿的持续基础补贴激励。
- $R_{\max}$ 防止罕见冲击或边缘情况导致发行量爆炸式增长。
- $\text{clip}(x, a, b) := \min(\max(x, a), b)$。

该更新在如下意义上是同态的：它仅依赖于协议可见量的比率，并在时间上以乘法方式组合：

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

受截断约束。

6.2 为何次线性（$\gamma < 1$）

若发行量与工作量呈线性比例（实际上相当于 $\gamma = 1$），W 的大幅增加可能造成失控激励，即挖矿增加带来等比例的发行量增加，从而破坏均衡稳定性。次线性响应（$\gamma < 1$）对此加以节制，保持负反馈机制。

6.3 启动期分量

我们假设一个持续衰减的启动期补贴：

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

其设计旨在吸引早期参与，同时避免离散减半冲击。该分量独立于自适应尾部，可参数化设定以比比特币更快地分配初始份额。

6.4 工作量比率信号的抗操纵性

设一名控制算力占比 μ 的矿工在第 $n-1$ 个区块压制参与量 ε，并在第 n 个区块恢复，从而抬高 W_n/W_{n-1}。

- 工作量比率约被抬高至 $(1-\varepsilon\mu)^{-1}$。
- 尾部发行增加量约为 $\Delta R \approx R_n^{\text{tail}} \cdot \varepsilon\mu\gamma$。
- 矿工获得的收益份额：$\mu^2\varepsilon\gamma R_n^{\text{tail}}$。
- 压制成本：$\varepsilon\mu \cdot P_n(R_n + (1-\beta)F_n)$。
- 只有当 $\mu\gamma R_n^{\text{tail}} > P_n(R_n + (1-\beta)F_n)$ 时，操纵才有利可图。
- 由于 $R_n^{\text{tail}} \le R_n$ 且 $\gamma < 1$，该阈值超过 γ，并随 $\gamma \to 0$ 趋近于 1。因此，次线性响应提供了抗操纵性，且随 γ 减小而增强。

7 固定手续费销毁与燃烧发言

7.1 固定手续费销毁

令 $\beta \in (0,1)$ 为协议常数（无预言机，无治理调整）。对于每个区块：

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

这使得矿工自发垃圾邮件" 回收" 不再是零成本，因为一部分手续费被销毁。

7.2 燃烧发言作为内生汇

令 $\mathcal{S}_n$ 表示第 n 个区块中" 发言" 事件（帖子、消息、推广交易）的集合，每个事件的销毁量 $b_i \ge 0$。定义：

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

注意力分配由关于 b_i 的单调规则控制（例如排名排序、比例分配或拍卖）。燃烧发言机制在 [4] 中被正式规定为一种联邦式反垃圾邮件消息协议，其中提供了完整的应用层实现，包括支付证明构造、

中继服务器验证以及发布-订阅广播。重要的是，b_i 以币为单位选择。外部价格（美元）仅通过自愿市场参与影响行为：若币在外部变得更便宜，广告商可以获取并销毁更多币来竞争同等的注意力，从而在无需任何预言机的情况下增加 B_n^{b2s}。随着网络价值随用户采用呈超线性增长 [9]，燃烧发言的需求可能以超线性速度随用户数量增长，提供一个随采用规模自然增强的内生汇。

需求模型。令 $D(P_n)$ 表示外部价格 P_n 下的以币计价的总销毁需求。N 个广告商各持有固定法币预算 b，每人将其兑换成币并销毁：$B_n^{\mathrm{b2s}} \approx Nb/P_n$。当 P_n 下跌时，以币计价的销毁量成比例上升——汇在价格下跌时增强，这正是负反馈所需的方向。这种法币预算机制使销毁需求在币单位上缺乏弹性而在法币单位上富有弹性，在无需任何预言机的情况下提供内生的稳定响应。

8 基于期望值的均衡草图

我们从期望值角度进行定性推理。

假设（如标准无许可安全性论证 [3] 所述）长期工作量供给锚定于外部单位中矿工的预期收益：

$$\mathbb{E}[W_n] \ \text{ 随 } \ \mathbb{E}[P_n] \cdot \mathbb{E}[R_n + F_n^{\mathrm{miner}}] \text{ 增加而增加。}$$

我们强调，P_n 和 k_e^* 并非预言机输入；它们仅出现在设计时校准和经济解释中。

所提出的机制将以下因素耦合：

- 工作量更高 $\Rightarrow$ 尾部发行量更高（次线性），
- 外部价格下跌 $\Rightarrow$ 在给定外部营销预算下，以币计价的竞争性燃烧发言增加，
- 手续费销毁 $\Rightarrow$ 即使在矿工控制下也存在持续的汇和反垃圾邮件成本。

因此期望值中的净供应变化为：

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

伪稳定性通过负反馈机制来寻求，其中：

- 需求快速增长抬高 P_n 和 W_n，
- 尾部规则次线性地增加发行量（抑制价格飙升），
- 燃烧发言和手续费销毁提供随使用量/注意力竞争增长的汇，
- 两者结合减少了极端稀缺驱动的波动性，同时保留了工作量证明安全激励。

我们不声称实现完美稳定性；所声称的是该系统具有内生的稳定倾向，而无需机构测量。与权益证明系统（验证者可以通过复杂的基础设施竞赛优化最大可提取价值（MEV）） [6, 7] 不同，工作量证明矿工面临本质上有限的优化机会，从而减少了安全支出向不透明渠道的位移。

8.1 冲击特征

处理良好的冲击：技术的渐进改进（k_e^* 的长期下降）和需求增长均通过工作量信号传导，使尾部规则能够按比例响应。

处理不佳的冲击：突发性能源价格不连续变动会在 W_n 没有立即可见变化的情况下改变 k_e^*，在难度调整之前形成一个失衡窗口。突发性大幅算力跳升（新一代矿机的出现）可能瞬时将 W_n/W_{n-1} 推出稳定机制；截断边界 $(R_{\min}, R_{\max})$ 限制但不能消除这种风险敞口。

这些局限性是无预言机设计的固有特征。相关比较基准不是信息完备的规划者，而是自由裁量治理——后者通过委员会决策响应冲击，但有其自身的公信力和俘获风险。

关于能源价格波动性的说明。伪稳定性目标是相对于能源成本的稳定性，而非相对于法币的稳定性。能源价格本身具有相当大的波动性（例如，2022 年天然气价格波动约 5 倍）。因此，该币将继承残余的能源价格方差。这是无预言机约束的设计后果：能源是植根于物理学的真实热力学成本，不像委员会定义的消费篮子。系统设计者不应期望法币价格稳定作为直接输出；预期结果是相对于固定供应机制减少极端稀缺驱动的波动性，而非硬钉住汇率。

8.2 线性化动态下的形式稳定性分析

我们对双环机制在均衡附近给出基于李雅普诺夫的稳定性论证。

设置。定义均衡三元组 (R^*, W^*, P^*)，满足挖矿均衡与供应平衡条件：

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

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

其中 k_e 为单位工作量的边际能源成本，N 与 b 为第 7.2节需求模型中的广告商数量与法币预算。设对均衡的对数偏差为：

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

线性化动态。在三个简化假设下：(i) 截断在均衡附近不活跃；(ii) 算力瞬时调整使矿工收益等于边际成本（$W_n k_e = P_n R_n^{\text{tail}}$），一阶近似给出 $w_n = p_n + r_n$；(iii) 价格以灵敏度 $\phi > 0$ 响应净供应偏差，即 $p_{n+1} \approx (1-\phi)p_n - \phi r_n$；代入得到工作偏差的自治二阶递推关系：

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

均衡附近的净供应偏差满足 $\Delta S_n/S \approx r_n + p_n = w_n$，故 $w_n \to 0$ 意味着净发行量趋于零。

定理 1 (双环机制的李雅普诺夫稳定性)**.** *若 $\phi \in (0, 2+2\gamma)$，则递推关系 (1)的特征根严格位于单位圆内，且以下结论成立：*

1. *存在正定二次李雅普诺夫函数 $V_n = \mathbf{w}_n^\top P\, \mathbf{w}_n$（其中 $\mathbf{w}_n = (w_n, w_{n-1})^\top$），满足对某 $\eta > 0$ 有 $\Delta V_n \le -\eta\, V_n$；*

2. *w_n 以几何速率趋于零；因此净供应偏差 $\Delta S_n/S \to 0$；*

3. r_n 收敛至有限极限 r_∞，且 $p_n \to -r_\infty$（价格稳定至与新水平供应平衡一致的值）。

证明. 递推关系 (1)的特征多项式为 $\chi(\lambda) = \lambda^2 - (1-\phi+\gamma)\lambda + \gamma$，系数 $a_1 = -(1-\phi+\gamma)$，$a_0 = \gamma$。离散时间系统的朱里稳定判据要求：(i) $|a_0| < 1$；(ii) $\chi(1) > 0$；(iii) $\chi(-1) > 0$。逐一验证：

- $|a_0| = \gamma < 1$，因 $\gamma \in (0,1)$。✓
- $\chi(1) = 1 - (1-\phi+\gamma) + \gamma = \phi > 0$，因 $\phi > 0$。✓
- $\chi(-1) = 1 + (1-\phi+\gamma) + \gamma = 2 + 2\gamma - \phi > 0$，当且仅当 $\phi < 2 + 2\gamma$。✓

在 $\phi \in (0, 2+2\gamma)$ 下，所有条件满足，故两个特征根均满足 $|\lambda_i| < 1$。

对于具有伴随矩阵 $A = \left(\begin{smallmatrix} 1-\phi+\gamma & -\gamma \\ 1 & 0 \end{smallmatrix}\right)$ 的任意稳定线性系统，离散李雅普诺夫方程 $A^\top P A - P = -I$ 存在唯一正定解 P [14]。相应的二次型 $V_n = \mathbf{w}_n^\top P\, \mathbf{w}_n$ 满足 $\Delta V_n = -\mathbf{w}_n^\top \mathbf{w}_n \le -\lambda_{\min}(P)^{-1} V_n$，故 $\eta = \lambda_{\min}(P)^{-1} > 0$。

w_n 的几何衰减蕴含 $\sum_n |w_n - w_{n-1}| < \infty$；由于 $r_{n+1} - r_n = \gamma(w_n - w_{n-1})$，级数 $r_n = r_0 + \gamma \sum_{k<n}(w_k - w_{k-1})$ 绝对收敛。极限满足 $r_\infty + p_\infty = \lim_n w_n = 0$。 □

注记（稳定性条件的经济解读）。上界 $\phi < 2 + 2\gamma$ 限制了价格对供应失衡的响应幅度。若价格灵敏度过高，尾部发行与价格反馈的组合将发生超调，产生振荡。次线性指数 γ 拓宽了稳定区间：较小的 γ（更保守的发行响应）收窄该区间，但同时提高了抗操纵性（第 6.4节）。这些权衡关系应指导参数校准。

注记（价格水平不确定性）。定理 1保证收敛至某个供应平衡均衡 $(R_\infty^{\text{tail}}, P_\infty)$，而非特定参考对 (R^*, P^*)。这反映了供应平衡货币模型中标准的价格水平不确定性：均衡水平依赖于初始条件，而均衡方差是有界的。

论证范围。形式证明适用于理想化假设下的均衡附近线性化系统。非线性效应、离散减半冲击与截断边界饱和超出本论证范围；其效应通过第 12节中的仿真加以处理。

9 实现注记（比特币风格守护进程）

9.1 无需铸币交易查找

R_n^{tail} 被定义为仅补贴部分（不含手续费）。节点在链状态/索引中将 R_n^{tail} 作为共识状态变量维护，从以下数据确定性计算：

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

在验证过程中，强制执行：

$$\text{铸币区块补贴} \le R_n^{\text{boot}} + R_n^{\text{tail}},$$

而手续费按惯例处理（根据共识规则应用固定销毁比例）。

9.2 仅区块头工作代理

W_n 直接从 `nBits`（目标位）推导，因此只需要最近的区块头，无需全历史扫描。

9.3 定点算术

为避免浮点不确定性，使用定点有理近似实现 $(W_n/W_{n-1})^\gamma$；对于 $\gamma = \frac{1}{2}$，整数平方根方法简单且稳定。

10 讨论：采用与非强制性启动

该设计是非强制性的：需求来源于自愿效用。燃烧发言需要注意力平台；因此，实际的启动路径是在注意力已经稀缺的领域（社区、出版、易受垃圾邮件侵扰的论坛）部署该系统，从而使销毁具有即时效用。CashWeb [4] 恰好提供了这样的应用层：一种联邦式消息协议，其中燃烧发言机制同时在应用层发挥反垃圾邮件作用，并在货币层发挥内生供应汇的作用。因此，在 CashWeb 消息网络中部署可在单一系统中同时引导效用和货币稳定性。加速启动份额可吸引早期参与，而长期动态则由尾部发行 + 销毁双环路而非持续稀缺冲击来主导。

冷启动阶段。定理 1的稳定性保证假设销毁需求非零；在燃烧发言活动可忽略的冷启动阶段不适用。在此阶段，汇环路实际上不活跃，发行量主要由 R_n^{boot} 决定。冷启动不是故障模式，而是一个已知的设计阶段：启动分量的规模正是为了在应用层网络效应积累期间维持挖矿参与。当销毁需求足以实质性抵消发行量时，稳定性保证生效——该阈值应在参数校准阶段根据预期的早期采用者数量进行估算。

11 参数推导与校准（数值选择延后确定）

本节推导关键参数的选择方法，基于参考均衡点。数值有意推迟到实现阶段确定，因为它们取决于硬件效率、当前电价、期望的基线安全性以及预期的”成熟”运行机制。

11.1 参考均衡

固定目标外部价格水平 P^*（例如 $P^* = \$0.01$ 每币，即每美元 100 币），以及由以下参数刻画的参考运行点：

- W^*：每区块的参考工作代理（从区块头难度/目标推导），
- k_e^*：每单位工作的边际外部成本（美元/W 单位），解释为边际矿工的电费加硬件运营支出，
- F^*：每区块的参考手续费量（以币计），
- β：固定手续费销毁比例（协议常数）。

令矿工获得的手续费分量为 $(1-\beta)F^*$，总补贴为

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

一阶均衡条件将每区块的预期外部矿工收益与边际外部成本相等：

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

求解所需总补贴得：

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

给定该时期所选择的启动期计划值 $R^{\text{boot},*}$，隐含的尾部水平为：

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

11.2 初始化和约束尾部状态

有状态尾部规则

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

不需要单独的缩放常数。取而代之，选择：

- 初始状态 R_0^{tail}（例如设定为接近预期启动机制下的 $R^{\text{tail},*}$），
- 正下界 $R_{\min} > 0$，以在需求崩溃时保持基础挖矿激励，
- 可选上界 $R_{\max}$，作为应对罕见冲击或极端情况的安全不变量。

实践中，$R_{\min}$ 可规定为参考尾部水平的一个分数，$R_{\min} = \eta R^{\text{tail},*}$，其中 $\eta \in (0,1)$，而 $R_{\max}$ 可设置为" 足够大" 或作为明确的不变量处理。所有此类数值选择均推迟至实现和实证测试阶段确定。

11.3 次线性指数的选择

指数 $\gamma \in (0,1)$ 控制响应度并避免线性于工作量的失控激励。自然候选值为 $\gamma = \frac{1}{2}$（平方根），但协议可在经过仿真和对抗性分析后，在实现阶段将 γ 选定为固定常数。

11.4 解读

上述校准方程在 (i) 期望的外部价格机制 P^* 与 (ii) 给定外部能源/硬件成本的预期基线安全/工作机制 W^* 之间提供了桥梁。协议本身不观测 P^* 或 k_e^*；这些是设计时校准量，仅用于选择初始常数。

12 仿真与验证清单

在部署之前，以下仿真足以验证定性行为并约束参数选择。不需要外部预言机。

- **参数扫描**：遍历 $\gamma \in (0,1)$（重点关注 $\gamma = \frac{1}{2}$）、手续费销毁比例 β、尾部下界 $R_{\min}$ 以及初始尾部状态 R_0^{tail}。
- **需求冲击**：对交易需求和燃烧发言活动施加阶跃和脉冲冲击；观测 R_n^{tail} 和净发行量 ΔS_n 的收敛情况。

- **挖矿冲击**：模拟可用算力的突发增加/减少（例如新一代矿机的出现），并验证在次线性规则下发行量响应的有界性。
- **对抗性场景**：建模矿工自发垃圾邮件尝试、手续费回收以及临时挖矿骚扰，以确认固定手续费销毁施加了不可约的成本。
- **长期饱和**：保持用户/活动代理不变，验证发行量收敛至稳态机制而非线性增长。
- **数值稳定性**：验证定点算术边界和截断不变量，确保跨实现的确定性行为。

这些仿真旨在验证稳定性和激励结构，而非预测精确的价格轨迹。

13 结论

本文规定了一种基于工作量证明的货币机制：(i) 仅使用协议可见的工作量信号进行自适应尾部发行，(ii) 通过手续费销毁和燃烧发言纳入无预言机的销毁汇。所得系统旨在通过将发行量和销毁与对抗性揭示的工作量及内生注意力竞争相耦合来实现相对能源的伪稳定性，从而避免自由裁量发行和机构测量。这一方法展示了对抗性成本揭示如何在算法货币政策设计中替代委员会管理的价格指数。进一步的工作应在明确的行为假设下正式化稳定性条件，并探索 γ、$(R_{\min}, R_{\max})$ 以及 β 的参数机制。

参考文献

[1] Bureau of Labor Statistics. 消费者价格指数中的享乐质量调整. 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. 走向更精确的生活成本衡量：咨询委员会关于消费者价格指数研究的最终报告（致参议院财政委员会）. U.S. Senate Finance Committee, 1996. `https://www.ssa.gov/history/reports/boskinrpt.html`

[3] E. Budish. 比特币与区块链的经济极限. *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. 闪电男孩 2.0：去中心化交易所中的抢先交易、交易重排序与共识不稳定性. *2020 IEEE Symposium on Security and Privacy*, pages 910–927, 2020.

[7] Flashbots Research. MEV-Explore：最大可提取价值活动实时仪表盘. `https://explore.flashbots.net/`, 2021.

[8] D. E. Lebow and J. B. Rudd. 消费者价格指数中的测量误差：现状如何？. *Journal of Economic Literature*, 41(1):159–201, 2003.

[9] B. Metcalfe. 梅特卡夫定律：网络随着用户数量的增加而变得更有价值. *Infoworld*, 17(40):53–54, 1995.

[10] S. Nakamoto. 比特币：一种点对点的电子现金系统. 2008. `https://bitcoin.org/bitcoin.pdf`

[11] N. Plassaras. 监管数字货币：将比特币纳入国际货币基金组织的管辖范围. *Chicago Journal of International Law*, 14(1):377–407, 2013.

[12] P. Todd. 令人惊讶的是，尾部发行并不导致通货膨胀. 2022. `https://petertodd.org/2022/surprisingly-tail-emission-is-not-inflationary`

[13] E. Weinstein. 对抗性测量与信息经济. The Portal with Eric Weinstein, 2021.

[14] H. K. Khalil. 非线性系统，第三版. Prentice Hall, 2002. （离散时间李雅普诺夫理论：定理 4.7 及相关内容。）