Chính sách tiền tệ PoW thích ứng không cần Oracle: Cơ chế xây dựng đạt giả ổn định thông qua phát hành đuôi kết hợp công việc và đốt tiền

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

Ngày 21 tháng 2 năm 2026
Version 1.1

Tóm tắt nội dung

Bài báo này đề xuất một phương án thay thế mang tính xây dựng cho Bitcoin, vừa giữ lại Bằng chứng Công việc (Proof-of-Work) vừa đạt được giả ổn định mà không cần dựa vào quản trị tùy ý hay oracle giá bên ngoài, đồng thời cung cấp một phương án đối lập với các chỉ số do ủy ban quản lý như CPI vốn phụ thuộc vào phương pháp luận chủ quan và đo lường thể chế. Dựa trên quan sát rằng PoW tiết lộ chi phí bảo mật có thể nhìn thấy từ giao thức thông qua độ khó [**?**] (và do đó là công việc dự kiến mỗi khối), chúng tôi xác định một cơ chế hai vòng lặp: (i) quy tắc phát hành đuôi thích ứng kết hợp công việc, được định nghĩa hoàn toàn từ các biến quan sát được từ tiêu đề khối và trạng thái đồng thuận trước đó; (ii) cơ chế đốt tiền theo thị trường (đốt-để-nói [**?**] và đốt một phần phí giao dịch) cung cấp bể hấp thụ cầu nội sinh mà không cần oracle nào. Thiết kế được biểu diễn theo kỳ vọng và sử dụng các phương trình cập nhật đồng cấu (dựa trên tỷ lệ) để tránh gián đoạn và giảm khả năng bị thao túng. Chúng tôi phác thảo một luận điểm ổn định dựa trên phản hồi âm giữa công việc, phát hành, nhu cầu đốt và giá cân bằng, đồng thời thảo luận về khả năng triển khai trong kiến trúc daemon và xác thực theo kiểu Bitcoin.

1 Mục tiêu thiết kế và tập ràng buộc

1.1 Mục tiêu: giả ổn định so với năng lượng

Chúng tôi tìm kiếm giả ổn định tương đối so với năng lượng (và do đó, gián tiếp so với các tài sản thực tương đối ổn định khác như USD), mà không cố gắng neo cứng tỷ giá. Mục đích là thực tế: giảm biến động đủ để các tác nhân chi phí cố định (lương, chuỗi cung ứng, hợp đồng nợ) có thể sử dụng đồng tiền mà không cần liên tục định giá lại.

1.2 Các ràng buộc

- **Không có oracle bên ngoài.** Không có CPI, không có nguồn cấp USD, không có chỉ số do ủy ban xác định.

- **Không có kiểm soát tùy ý.** Các tham số tiền tệ không nên là đòn bẩy chiến lược cho bất kỳ nhóm nào.
- **PoW được giữ lại.** Độ khó/công việc được coi là tín hiệu chi phí bảo mật có thể nhìn thấy từ giao thức.
- **Áp dụng không cưỡng ép.** Nhu cầu phải xuất phát từ tính hữu ích tự nguyện và cạnh tranh thị trường.

2 Ký hiệu

Lập chỉ mục các khối theo chiều cao n.

Đặt:

- P_n: giá bên ngoài của đồng tiền (ví dụ USD/đồng tiền), được coi là biến ẩn (không phải đầu vào oracle).
- R_n^{boot}: thành phần trợ cấp khởi động (đồng tiền/khối), được xác định trước, suy giảm liên tục.
- R_n^{tail}: thành phần trợ cấp đuôi thích ứng (đồng tiền/khối), biến trạng thái giao thức.
- F_n: phí giao dịch (đồng tiền/khối).
- B_n: đồng tiền bị đốt trong khối n bởi đốt phí và đốt-để-nói (đồng tiền/khối).

Tổng trợ cấp coinbase là:

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

Tổng phát hành ròng trong khối n là:

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

lưu ý rằng trong kế toán kiểu Bitcoin, phí là các khoản chuyển cho thợ đào trừ khi được đốt một cách rõ ràng.

3 Proxy công việc từ các bit tiêu đề: Độ khó và số lần băm dự kiến

Đặt T_n là mục tiêu PoW được ngụ ý bởi trường tiêu đề khối `nBits` tại chiều cao n.

Định nghĩa độ khó (tương đối so với mục tiêu tham chiếu T_0):

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

Định nghĩa số lần băm dự kiến mỗi khối theo oracle băm đồng nhất:

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

(theo quy ước hệ số hằng số chuẩn).

Cả hai đều tỷ lệ thuận với nghịch đảo của mục tiêu:

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

Do đó chúng tôi định nghĩa một proxy công việc trừu tượng, có thể nhìn thấy từ giao thức W_n và cho phép một trong hai:

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

với sự hiểu biết rằng lựa chọn này chỉ ảnh hưởng đến các hằng số tỷ lệ, không ảnh hưởng đến động lực định tính.

4 Chỉ số giá thể chế so với tiết lộ chi phí đối lập

4.1 Vấn đề đo lường CPI

Các hệ thống đo lường giá thể chế như Chỉ số Giá Tiêu dùng phải đối mặt với những thách thức được ghi chép đầy đủ ảnh hưởng đến độ tin cậy của chúng trong các ứng dụng chính sách tiền tệ. Ủy ban Boskin [**?**] đã xác định sai lệch tăng có hệ thống trong đo lường CPI của Hoa Kỳ, ước tính mỗi năm bị báo cáo quá mức 1,1 điểm phần trăm do các hạn chế phương pháp luận bao gồm sai lệch thay thế, sai lệch kênh bán lẻ, sai lệch chất lượng và sai lệch sản phẩm mới. Phân tích tiếp theo của Lebow và Rudd [**?**] xác nhận sai số đo lường dai dẳng bất chấp các cải tiến kỹ thuật, lưu ý rằng độ trễ sửa đổi và điều chỉnh chất lượng chủ quan đưa ra sự không chắc chắn ảnh hưởng đến các quyết định chính sách thời gian thực.

Việc xây dựng CPI hiện đại kết hợp các yếu tố tùy ý rộng rãi thông qua điều chỉnh chất lượng hedonic [**?**], trong đó các cơ quan thống kê đưa ra các xác định chủ quan về giá "thực sự" của hàng hóa và dịch vụ đang phát triển. Các lựa chọn phương pháp luận dựa trên ủy ban—chẳng hạn như tổng hợp bình quân hình học so với số học, tham số điều chỉnh theo mùa và các thủ tục chuẩn hóa chất lượng—nhúng phán đoán thể chế có thể không phản ánh nhận thức của những người tham gia thị trường về những thay đổi trong sức mua.

4.2 Tiết lộ chi phí đối lập như một phương án thay thế

Đo lường dựa trên PoW cung cấp một phương án thay thế mang tính cấu trúc dựa trên tiết lộ chi phí đối lập thay vì đồng thuận ủy ban. Trong khi các chỉ số thể chế đòi hỏi tổng hợp chủ quan giá giỏ hàng và đánh giá chất lượng, tín hiệu dựa trên công việc bắt nguồn từ các quyết định chi tiêu thực tế của thợ đào dưới áp lực cạnh tranh. Cơ chế điều chỉnh độ khó tự nhiên kết hợp chi phí công nghệ thay đổi, giá năng lượng và hiệu quả vốn mà không cần điều chỉnh chất lượng rõ ràng hay quyết định ủy ban phương pháp luận.

Cách tiếp cận đối lập này, xây dựng dựa trên khung chống chiếm đoạt thể chế của Weinstein [**?**], tận dụng thực tế rằng các thợ đào không thể phối hợp để cố tình báo cáo sai cấu trúc chi phí của họ mà không mất lợi thế cạnh tranh. Không giống như thu thập giá dựa trên khảo sát hay

điều chỉnh chất lượng được xác định hành chính, proxy công việc xuất hiện từ cạnh tranh kinh tế thực sự, nơi báo cáo sai mang hậu quả tài chính tức thì.

Điều quan trọng là, đo lường dựa trên PoW tránh được các vấn đề độ trễ thời gian và sửa đổi ảnh hưởng đến các chỉ số thể chế. Trong khi các con số CPI trải qua sửa đổi đáng kể khi có dữ liệu tốt hơn, độ khó blockchain tự động điều chỉnh dựa trên hành vi đào thực tế, cung cấp tiết lộ tín hiệu chi phí thời gian thực mà không cần dựa vào dữ liệu khảo sát chậm trễ hay hiệu chỉnh thống kê tiếp theo.

4.3 Ý nghĩa đối với chính sách tiền tệ

Sự phân biệt giữa đo lường do ủy ban quản lý và đo lường được tiết lộ đối lập trở nên đặc biệt quan trọng đối với các cơ chế tiền tệ hoạt động mà không có giám sát tùy ý. Trong khi chính sách tiền tệ truyền thống có thể điều chỉnh theo sửa đổi CPI và cập nhật phương pháp luận thông qua can thiệp ngân hàng trung ương, các hệ thống thuật toán đòi hỏi đầu vào đo lường vừa kịp thời vừa chống thao túng.

Cơ chế kết hợp công việc được đề xuất đại diện cho một triển khai của nguyên tắc đo lường đối lập này: thay vì theo dõi các chỉ số giá bên ngoài nhúng các lựa chọn phương pháp luận thể chế, hệ thống phản hồi với các tín hiệu chi phí xuất hiện một cách cơ học từ hoạt động đào cạnh tranh. Cách tiếp cận này đánh đổi chiều rộng của các chỉ số sức mua truyền thống để đổi lấy khả năng chống giả mạo và tính sẵn có thời gian thực của chi phí công việc được tiết lộ đối lập.

5 Tổng quan cơ chế: Hai vòng lặp kết hợp

Cơ chế có hai thành phần kết hợp:

5.1 (A) Phát hành đuôi thích ứng (vòng lặp nguồn)

Phát hành đuôi kết hợp công việc dưới tuyến tính điều chỉnh tỷ lệ phát hành dài hạn chỉ sử dụng (W_n, W_{n-1}) và trạng thái đuôi trước đó R_n^{tail}.

5.2 (B) Đốt thị trường (vòng lặp bể hấp thụ)

Đồng tiền bị phá hủy thông qua:

- **Đốt phí một phần:** một phần cố định phí giao dịch bị đốt.
- **Đốt-để-nói:** người dùng cạnh tranh đốt đồng tiền để mua sự chú ý khan hiếm hoặc ưu tiên đăng bài, chỉ được định giá bằng đơn vị đồng tiền (không có oracle).

6 Quy tắc phát hành đuôi thích ứng

6.1 Cập nhật đồng cấu dưới tuyến tính

Đặt $\gamma \in (0, 1)$ là số mũ hằng số; chúng tôi nhấn mạnh $\gamma = \frac{1}{2}$ (căn bậc hai) là ứng cử viên tự nhiên.

Định nghĩa cập nhật có trạng thái:

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

trong đó:

- $R_{\min} > 0$ đảm bảo ưu đãi trợ cấp cơ sở liên tục cho hoạt động đào.
- $R_{\max}$ ngăn chặn các cú sốc hiếm gặp hoặc các trường hợp biên làm phát sinh phát hành bùng nổ.
- $\text{clip}(x, a, b) := \min(\max(x, a), b)$.

Cập nhật này là *đồng cấu* theo nghĩa nó chỉ phụ thuộc vào tỷ lệ của các đại lượng có thể nhìn thấy từ giao thức và kết hợp theo phép nhân theo thời gian:

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

tùy thuộc vào kẹp.

6.2 Tại sao dưới tuyến tính ($\gamma < 1$)

Nếu phát hành tỷ lệ tuyến tính với công việc (thực tế là $\gamma = 1$), các tăng lớn trong W có thể tạo ra ưu đãi mất kiểm soát, nơi tăng đào tạo ra tăng phát hành theo tỷ lệ, làm mất ổn định cân bằng. Phản hồi dưới tuyến tính ($\gamma < 1$) điều tiết điều này, duy trì chế độ phản hồi âm.

6.3 Thành phần khởi động

Chúng tôi giả định một trợ cấp khởi động suy giảm liên tục:

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

được chọn để thu hút sự tham gia sớm mà không có các cú sốc giảm một nửa rời rạc. Thành phần này độc lập với đuôi thích ứng và có thể được tham số hóa để phân phối một phần ban đầu nhanh hơn Bitcoin.

6.4 Khả năng chống thao túng của tín hiệu tỷ lệ công việc

Đặt một thợ đào kiểm soát phần μ hashpower giảm sự tham gia bởi ε trong khối $n-1$ và khôi phục nó trong khối n, thổi phồng W_n/W_{n-1}.

- Tỷ lệ công việc thổi phồng xấp xỉ $(1 - \varepsilon\mu)^{-1}$.
- Phát hành đuôi tăng bởi $\Delta R \approx R_n^{\text{tail}} \cdot \varepsilon\mu\gamma$.
- Phần lợi nhuận của thợ đào: $\mu^2\varepsilon\gamma R_n^{\text{tail}}$.
- Chi phí giảm thiểu: $\varepsilon\mu \cdot P_n(R_n + (1-\beta)F_n)$.

- Thao túng chỉ có lợi khi $\mu\gamma R_n^{\text{tail}} > P_n(R_n + (1-\beta)F_n)$.
- Vì $R_n^{\text{tail}} \le R_n$ và $\gamma < 1$, ngưỡng này vượt quá γ và tiếp cận 1 khi $\gamma \to 0$. Do đó, phản hồi dưới tuyến tính cung cấp khả năng chống thao túng tăng chặt khi γ giảm.

7 Đốt phí cố định và đốt-để-nói

7.1 Đốt phí cố định

Đặt $\beta \in (0,1)$ là hằng số giao thức (không có oracle, không điều chỉnh quản trị). Cho mỗi khối:

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

Điều này ngăn "tái chế" spam của thợ đào không có chi phí, vì một phần phí bị phá hủy.

7.2 Đốt-để-nói như một bể hấp thụ nội sinh

Đặt $\mathcal{S}_n$ ký hiệu một tập hợp các sự kiện "nói" (bài đăng, tin nhắn, giao dịch được quảng bá) trong khối n, mỗi sự kiện có lượng đốt $b_i \ge 0$. Định nghĩa:

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

Phân bổ sự chú ý được quản lý bởi một quy tắc đơn điệu trong b_i (ví dụ xếp hạng, chia sẻ theo tỷ lệ hoặc đấu giá). Cơ chế đốt-để-nói được chính thức hóa như một giao thức nhắn tin liên kết chống spam trong [**?**], cung cấp triển khai lớp ứng dụng hoàn chỉnh bao gồm xây dựng bằng chứng thanh toán, xác minh máy chủ relay và phát sóng publish-subscribe. Quan trọng là, b_i được chọn bằng đơn vị đồng tiền. Giá bên ngoài (USD) chỉ ảnh hưởng đến hành vi thông qua sự tham gia thị trường tự nguyện: nếu đồng tiền trở nên rẻ hơn bên ngoài, các nhà quảng cáo có thể mua và đốt nhiều đồng tiền hơn để cạnh tranh cùng sự chú ý, tăng B_n^{b2s} mà không cần oracle nào. Khi giá trị mạng tăng theo tuyến tính siêu với việc áp dụng của người dùng [**?**], nhu cầu đốt-để-nói có thể tăng nhanh hơn tuyến tính theo số lượng người dùng, cung cấp bể hấp thụ tự nhiên mạnh lên theo việc áp dụng.

Mô hình nhu cầu. Đặt $D(P_n)$ ký hiệu nhu cầu đốt theo đồng tiền tổng hợp tại giá bên ngoài P_n. Với N nhà quảng cáo mỗi người giữ ngân sách fiat cố định b, mỗi người chuyển đổi thành đồng tiền và đốt: $B_n^{\text{b2s}} \approx Nb/P_n$. Khi P_n giảm, lượng đốt theo đồng tiền tăng theo tỷ lệ—bể hấp thụ mạnh lên khi giá giảm, đây là hướng cần thiết cho phản hồi âm. Cơ chế ngân sách fiat này làm cho nhu cầu đốt không co giãn theo đơn vị đồng tiền và co giãn theo đơn vị fiat, cung cấp phản hồi ổn định nội sinh mà không cần oracle nào.

8 Phác thảo cân bằng dựa trên kỳ vọng

Chúng tôi lý luận định tính theo kỳ vọng.

Giả sử (như trong các luận điểm bảo mật không cần phép tiêu chuẩn [**?**]) rằng việc cung

cấp công việc dài hạn được neo đậu với doanh thu dự kiến của thợ đào theo đơn vị bên ngoài:

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

Chúng tôi nhấn mạnh rằng P_n và k_e^* không phải là đầu vào oracle; chúng chỉ xuất hiện trong hiệu chỉnh thời gian thiết kế và diễn giải kinh tế.

Cơ chế được đề xuất kết hợp:

- công việc cao hơn ⇒ phát hành đuôi cao hơn (dưới tuyến tính),
- giá bên ngoài giảm ⇒ tăng đốt-để-nói cạnh tranh (theo đơn vị đồng tiền) với một ngân sách marketing bên ngoài nhất định,
- đốt phí ⇒ bể hấp thụ dai dẳng và chi phí chống spam ngay cả dưới sự kiểm soát của thợ đào.

Vì vậy, thay đổi nguồn cung ròng theo kỳ vọng là:

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

Giả ổn định được tìm kiếm thông qua chế độ phản hồi âm nơi:

- tăng trưởng nhu cầu nhanh nâng P_n và W_n,
- quy tắc đuôi tăng phát hành dưới tuyến tính (điều tiết đỉnh giá),
- đốt-để-nói và đốt phí cung cấp bể hấp thụ tăng theo sử dụng/cạnh tranh chú ý,
- sự kết hợp giảm biến động cực đoan do khan hiếm trong khi duy trì ưu đãi bảo mật PoW.

Không có tuyên bố về sự ổn định hoàn hảo; tuyên bố là hệ thống có xu hướng ổn định nội sinh mà không cần đo lường thể chế. Không giống như các hệ thống PoS nơi người xác thực có thể tối ưu hóa giá trị có thể chiết xuất tối đa (MEV) thông qua các cuộc đua cơ sở hạ tầng tinh vi [**?**, **?**], các thợ đào PoW phải đối mặt với cơ hội tối ưu hóa vốn hạn chế, giảm sự dịch chuyển chi phí bảo mật vào các kênh mờ đục.

8.1 Đặc trưng cú sốc

Các cú sốc được xử lý tốt: Cải tiến công nghệ dần dần (suy giảm thế tục trong k_e^*) và tăng trưởng nhu cầu đều di chuyển qua tín hiệu công việc, cho phép quy tắc đuôi phản hồi theo tỷ lệ.

Các cú sốc được xử lý kém: Gián đoạn giá năng lượng đột ngột làm thay đổi k_e^* mà không có sự thay đổi ngay lập tức có thể nhìn thấy trong W_n, tạo ra cửa sổ mất cân bằng trước khi độ khó điều chỉnh. Các cú nhảy hashrate lớn đột ngột (thế hệ ASIC mới) có thể tạm thời đẩy W_n/W_{n-1} ra khỏi chế độ ổn định; các giới hạn clip $(R_{\min}, R_{\max})$ chứa nhưng không loại bỏ sự phơi lộ này.

Những hạn chế này vốn có trong thiết kế không cần oracle. Phép so sánh liên quan không phải với người lập kế hoạch được thông tin đầy đủ mà với quản trị tùy ý, vốn phản hồi với các cú sốc thông qua quyết định ủy ban với rủi ro uy tín và chiếm đoạt riêng của nó.

Lưu ý về biến động giá năng lượng. Mục tiêu giả ổn định là sự ổn định *so với chi phí năng lượng*, không phải so với tiền fiat. Giá năng lượng thể hiện biến động đáng kể riêng của chúng (ví dụ, giá khí đốt tự nhiên dao động xấp xỉ 5 lần trong năm 2022). Do đó, đồng tiền sẽ thừa hưởng phương sai giá năng lượng còn lại. Đây là hệ quả thiết kế của ràng buộc không cần oracle: năng lượng là chi phí nhiệt động lực thực được neo đậu trong vật lý, không giống như giỏ tiêu dùng do ủy ban xác định. Các nhà thiết kế hệ thống không nên kỳ vọng sự ổn định giá fiat như một đầu ra trực tiếp; kết quả dự định là giảm biến động cực đoan do khan hiếm so với chế độ cung cố định, không phải neo cứng.

8.2 Phân tích ổn định chính thức theo động lực tuyến tính hóa

Chúng tôi cung cấp một luận điểm ổn định dựa trên Lyapunov cho cơ chế hai vòng lặp trong lân cận của cân bằng.

Thiết lập. Định nghĩa bộ ba cân bằng (R^*, W^*, P^*) thỏa mãn các điều kiện cân bằng đào và cân bằng cung:

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

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

Đây k_e là chi phí năng lượng biên trên mỗi đơn vị công việc và N, b là số lượng nhà quảng cáo và ngân sách fiat từ mô hình nhu cầu của Mục **??**. Đặt các độ lệch log từ cân bằng là:

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

Động lực tuyến tính hóa. Dưới ba giả định đơn giản hóa: (i) kẹp không hoạt động gần cân bằng; (ii) hashrate điều chỉnh ngay lập tức để cân bằng doanh thu thợ đào với chi phí biên ($W_n k_e = P_n R_n^{\text{tail}}$), cho $w_n = p_n + r_n$ theo bậc nhất; và (iii) giá phản hồi với độ lệch cung ròng với độ nhạy $\phi > 0$, tức là $p_{n+1} \approx (1-\phi)p_n - \phi r_n$; thay thế cho ra hệ thức truy hồi bậc hai tự trị cho độ lệch công việc:

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

Độ lệch cung ròng thỏa mãn $\Delta S_n/S \approx r_n + p_n = w_n$ gần cân bằng, vì vậy $w_n \to 0$ ngụ ý phát hành ròng biến mất.

Định lý 1 (Ổn định Lyapunov của Cơ chế Hai Vòng lặp)**.** *Nếu $\phi \in (0,\, 2+2\gamma)$, thì các nghiệm đặc trưng của hệ thức truy hồi (**??**) nằm hoàn toàn bên trong đĩa đơn vị, và các kết luận sau đây đúng:*

1. *Tồn tại hàm Lyapunov toàn phương xác định dương $V_n = \mathbf{w}_n^\top P\, \mathbf{w}_n$, trong đó $\mathbf{w}_n = (w_n,\, w_{n-1})^\top$, thỏa mãn $\Delta V_n \le -\eta\, V_n$ với một $\eta > 0$ nào đó;*
2. *$w_n \to 0$ theo cấp số nhân hình học; do đó độ lệch cung ròng $\Delta S_n/S \to 0$;*
3. *r_n hội tụ đến giới hạn hữu hạn r_∞, và $p_n \to -r_\infty$ (giá ổn định nhất quán với cân bằng cung ở mức mới).*

Chứng minh. Đa thức đặc trưng của (**??**) là $\chi(\lambda) = \lambda^2 - (1 - \phi + \gamma)\lambda + \gamma$, với các hệ số $a_1 = -(1-\phi+\gamma)$ và $a_0 = \gamma$. Tiêu chí ổn định Jury cho đa thức thời gian rời rạc bậc 2 yêu cầu: (i) $|a_0| < 1$; (ii) $\chi(1) > 0$; (iii) $\chi(-1) > 0$. Chúng tôi xác minh từng điều:

- $|a_0| = \gamma < 1$ vì $\gamma \in (0, 1)$. ✓
- $\chi(1) = 1 - (1 - \phi + \gamma) + \gamma = \phi > 0$ vì $\phi > 0$. ✓
- $\chi(-1) = 1 + (1 - \phi + \gamma) + \gamma = 2 + 2\gamma - \phi > 0$ khi và chỉ khi $\phi < 2 + 2\gamma$. ✓

Tất cả điều kiện đúng theo $\phi \in (0, 2 + 2\gamma)$, vì vậy cả hai nghiệm thỏa mãn $|\lambda_i| < 1$.

Với bất kỳ hệ tuyến tính ổn định nào với ma trận đồng hành A (trong đó $A = \left(\begin{smallmatrix} 1-\phi+\gamma & -\gamma \\ 1 & 0 \end{smallmatrix}\right)$), phương trình Lyapunov rời rạc $A^\top P A - P = -I$ cho nghiệm xác định dương duy nhất P [**?**]. Dạng toàn phương tương ứng $V_n = \mathbf{w}_n^\top P\, \mathbf{w}_n$ thỏa mãn $\Delta V_n = -\mathbf{w}_n^\top \mathbf{w}_n \le -\lambda_{\min}(P)^{-1} V_n$, vì vậy $\eta = \lambda_{\min}(P)^{-1} > 0$.

Suy giảm hình học của w_n ngụ ý $\sum_n |w_n - w_{n-1}| < \infty$; vì $r_{n+1} - r_n = \gamma(w_n - w_{n-1})$, chuỗi $r_n = r_0 + \gamma \sum_{k<n}(w_k - w_{k-1})$ hội tụ tuyệt đối. Giới hạn thỏa mãn $r_\infty + p_\infty = \lim_n w_n = 0$. □

Nhận xét (Diễn giải kinh tế của điều kiện ổn định). Giới hạn $\phi < 2 + 2\gamma$ hạn chế mức độ giá phản hồi tích cực với mất cân bằng cung. Nếu độ nhạy giá quá lớn, sự kết hợp phát hành đuôi và phản hồi giá vượt mục tiêu, tạo ra dao động. Số mũ dưới tuyến tính γ mở rộng vùng ổn định: γ nhỏ hơn (phát hành bảo thủ hơn) thu hẹp nó đồng thời cải thiện khả năng chống thao túng (Mục **??**). Những đánh đổi này nên thông báo cho việc hiệu chỉnh tham số.

Nhận xét (Sự bất định mức giá). Định lý **??** đảm bảo hội tụ đến *một* cân bằng cân bằng cung $(R_\infty^{\text{tail}}, P_\infty)$ nhưng không cụ thể đến cặp tham chiếu (R^*, P^*). Điều này phản ánh sự bất định mức giá tiêu chuẩn trong các mô hình tiền tệ cân bằng cung: *mức* cân bằng phụ thuộc vào điều kiện ban đầu, trong khi *phương sai* cân bằng bị giới hạn. Việc neo đậu ở một mức giá cụ thể sẽ đòi hỏi oracle hoặc chính sách tùy ý—bị loại trừ theo thiết kế.

Phạm vi của luận điểm. Bằng chứng chính thức áp dụng cho hệ tuyến tính hóa gần cân bằng theo các giả định lý tưởng hóa (điều chỉnh hashrate tức thì, kẹp không hoạt động, nhu cầu đốt ngân sách fiat). Các hiệu ứng phi tuyến, các cú sốc giảm một nửa rời rạc và bão hòa giới hạn clip nằm ngoài phạm vi của luận điểm này; tác động của chúng được giải quyết thông qua mô phỏng trong Mục **??**.

9 Ghi chú triển khai (daemon kiểu Bitcoin)

9.1 Không cần tra cứu coinbase

R_n^{tail} được định nghĩa là *chỉ trợ cấp* (không bao gồm phí). Các nút duy trì R_n^{tail} như một biến trạng thái đồng thuận trong chainstate/index, được tính toán xác định từ:

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

Trong quá trình xác thực, thực thi:

$$\text{trợ cấp coinbase} \le R_n^{\text{boot}} + R_n^{\text{tail}},$$

trong khi phí được xử lý như thường lệ (với tỷ lệ đốt cố định áp dụng theo quy tắc đồng thuận).

9.2 Proxy công việc chỉ tiêu đề

W_n được suy ra trực tiếp từ `nBits` (các bit mục tiêu), vì vậy chỉ cần các tiêu đề gần đây. Không cần quét toàn bộ lịch sử.

9.3 Số học điểm cố định

Để tránh không xác định tính toán điểm nổi, triển khai $(W_n/W_{n-1})^\gamma$ sử dụng xấp xỉ hữu tỷ điểm cố định; với $\gamma = \frac{1}{2}$, các phương pháp căn bậc hai nguyên đơn giản và ổn định.

10 Thảo luận: Áp dụng và khởi động không cưỡng ép

Thiết kế không cưỡng ép: nhu cầu xuất phát từ tính hữu ích tự nguyện. Đốt-để-nói đòi hỏi một bề mặt chú ý; do đó, con đường khởi động thực tế là triển khai hệ thống trong một miền nơi sự chú ý đã khan hiếm (cộng đồng, xuất bản, diễn đàn dễ bị spam) để việc đốt có tính hữu ích tức thì. CashWeb [**?**] cung cấp chính xác lớp ứng dụng như vậy: một giao thức nhắn tin liên kết trong đó cơ chế đốt-để-nói đồng thời hoạt động như ngăn chặn spam ở lớp ứng dụng và như bể hấp thụ cung nội sinh ở lớp tiền tệ. Do đó, triển khai trong mạng nhắn tin CashWeb khởi động cả tính hữu ích và ổn định tiền tệ trong một hệ thống duy nhất. Phần khởi động gia tốc có thể thu hút sự tham gia sớm, trong khi động lực dài hạn được quản lý bởi các vòng lặp đuôi+đốt thay vì các cú sốc khan hiếm liên tục.

Chế độ khởi động lạnh. Các đảm bảo ổn định của Định lý **??** giả định nhu cầu đốt khác không; chúng không áp dụng trong chế độ khởi động lạnh nơi hoạt động đốt-để-nói là không đáng kể. Trong giai đoạn này, vòng lặp bể hấp thụ thực tế không hoạt động và phát hành được quản lý bởi R_n^{boot} mà thôi. Khởi động lạnh không phải là chế độ thất bại mà là một giai đoạn thiết kế đã biết: thành phần khởi động được định kích thước chính xác để duy trì sự tham gia đào trong khi hiệu ứng mạng lớp ứng dụng tích lũy. Các đảm bảo ổn định trở nên hoạt động khi nhu cầu đốt đủ lớn để B_n^{b2s} bù đắp có nghĩa cho phát hành—một ngưỡng nên được ước tính trong quá trình hiệu chỉnh tham số dựa trên số lượng người áp dụng sớm dự kiến.

11 Suy ra tham số và hiệu chỉnh (Lựa chọn số học bị hoãn)

Mục này suy ra cách các tham số chính có thể được chọn từ một cân bằng tham chiếu. Các giá trị số học có chủ ý bị hoãn đến triển khai, vì chúng phụ thuộc vào hiệu quả phần cứng, giá điện hiện hành, bảo mật đường cơ sở mong muốn và chế độ hoạt động "trưởng thành" dự định.

11.1 Cân bằng tham chiếu

Cố định mức giá bên ngoài mục tiêu P^* (ví dụ $P^* = \$0.01$ mỗi đồng tiền, tức là 100 đồng tiền mỗi USD) và một điểm hoạt động tham chiếu được đặc trưng bởi:

- W^*: proxy công việc tham chiếu mỗi khối (suy ra từ độ khó/mục tiêu tiêu đề),

- k_e^*: chi phí bên ngoài biên trên mỗi đơn vị công việc (USD mỗi đơn vị W), được hiểu là điện+phần cứng OPEX trên thợ đào biên,
- F^*: khối lượng phí tham chiếu theo đồng tiền mỗi khối,
- β: tỷ lệ đốt phí cố định (hằng số giao thức).

Đặt thành phần phí nhận bởi thợ đào là $(1-\beta)F^*$, và tổng trợ cấp là

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

Điều kiện cân bằng bậc nhất cân bằng doanh thu thợ đào bên ngoài dự kiến mỗi khối với chi phí bên ngoài biên:

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

Giải cho tổng trợ cấp cần thiết cho:

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

Cho giá trị lịch biểu khởi động được chọn $R^{\text{boot},*}$ tại thời điểm đó, mức đuôi ngụ ý là:

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

11.2 Khởi tạo và giới hạn trạng thái đuôi

Quy tắc đuôi có trạng thái

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

không đòi hỏi một hằng số tỷ lệ riêng biệt. Thay vào đó, người ta chọn:

- trạng thái ban đầu R_0^{tail} (ví dụ đặt gần $R^{\text{tail},*}$ cho chế độ ra mắt dự định),
- sàn dương $R_{\min} > 0$ để duy trì ưu đãi đào cơ sở theo sự sụp đổ nhu cầu,
- tùy chọn giới hạn $R_{\max}$ như một bất biến an toàn chống lại các cú sốc hiếm gặp hoặc các trường hợp góc.

Trong thực tế, $R_{\min}$ có thể được xác định như một phần của mức đuôi tham chiếu, $R_{\min} = \eta R^{\text{tail},*}$ với một $\eta \in (0,1)$ nào đó, trong khi $R_{\max}$ có thể được đặt "đủ lớn" hoặc được coi là một bất biến rõ ràng. Tất cả các lựa chọn số học như vậy bị hoãn đến triển khai và kiểm thử thực nghiệm.

11.3 Chọn số mũ dưới tuyến tính

Số mũ $\gamma \in (0,1)$ quản lý khả năng phản hồi và tránh các ưu đãi mất kiểm soát tuyến tính theo công việc. Một ứng cử viên tự nhiên là $\gamma = \frac{1}{2}$ (căn bậc hai), nhưng giao thức có thể coi γ là một hằng số cố định được chọn trong quá trình triển khai sau mô phỏng và phân tích đối lập.

11.4 Diễn giải

Các phương trình hiệu chỉnh ở trên cung cấp cầu nối giữa (i) chế độ giá bên ngoài mong muốn P^* và (ii) chế độ bảo mật/công việc đường cơ sở dự định W^* cho trước chi phí năng lượng/phần cứng bên ngoài. Bản thân giao thức không quan sát P^* hay k_e^*; đây là các đại lượng hiệu chỉnh thời gian thiết kế chỉ được sử dụng để chọn các hằng số ban đầu.

12 Danh sách kiểm tra mô phỏng và xác thực

Trước khi triển khai, các mô phỏng sau là đủ để xác thực hành vi định tính và giới hạn các lựa chọn tham số. Không cần oracle bên ngoài.

- **Quét tham số:** Biến thiên $\gamma \in (0, 1)$ (nhấn mạnh vào $\gamma = \frac{1}{2}$), tỷ lệ đốt phí β, sàn đuôi $R_{\min}$, và trạng thái đuôi ban đầu R_0^{tail}.
- **Cú sốc nhu cầu:** Đưa ra các cú sốc bước và xung đến nhu cầu giao dịch và hoạt động đốt-để-nói; quan sát sự hội tụ của R_n^{tail} và phát hành ròng ΔS_n.
- **Cú sốc đào:** Mô phỏng các tăng/giảm đột ngột trong hashpower có sẵn (ví dụ thay đổi thế hệ ASIC) và xác minh phản hồi phát hành bị giới hạn theo quy tắc dưới tuyến tính.
- **Các tình huống đối lập:** Mô hình hóa các nỗ lực tự spam thợ đào, tái chế phí và ngăn chặn đào tạm thời để xác nhận đốt phí cố định áp đặt chi phí không thể giảm.
- **Bão hòa dài hạn:** Giữ các proxy người dùng/hoạt động cố định và xác minh rằng phát hành hội tụ đến chế độ ổn định thay vì tăng trưởng tuyến tính.
- **Ổn định số học:** Xác thực các giới hạn số học điểm cố định và các bất biến kẹp để đảm bảo hành vi xác định trên các triển khai.

Các mô phỏng này nhằm xác thực cấu trúc ổn định và ưu đãi hơn là dự đoán quỹ đạo giá chính xác.

13 Kết luận

Chúng tôi đã xác định một cơ chế tiền tệ dựa trên PoW (i) chỉ sử dụng tín hiệu công việc có thể nhìn thấy từ giao thức để phát hành đuôi thích ứng và (ii) kết hợp bể hấp thụ đốt không cần oracle thông qua đốt phí và đốt-để-nói. Hệ thống kết quả nhắm đến giả ổn định so với năng lượng bằng cách kết hợp phát hành và đốt với công việc được tiết lộ đối lập và cạnh tranh chú ý nội sinh, tránh phát hành tùy ý và đo lường thể chế. Cách tiếp cận này chứng minh cách tiết lộ chi phí đối lập có thể thay thế các chỉ số giá do ủy ban quản lý trong thiết kế chính sách tiền tệ thuật toán. Công việc tiếp theo nên chính thức hóa các điều kiện ổn định theo các giả định hành vi rõ ràng và khám phá các chế độ tham số cho γ, $(R_{\min}, R_{\max})$ và β.

Tài liệu

[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.)