Chi Tiêu Bảo Mật, Năng Lượng và Tính Minh Bạch của Phát Hành trong Đồng Thuận Không Cần Cấp Phép

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

Ngày 21 tháng 2 năm 2026
Version 1.1

Tóm tắt nội dung

Các hệ thống Bằng Chứng Cổ Phần (PoS) thường được mô tả là giải pháp thay thế thân thiện với môi trường so với Bằng Chứng Công Việc (PoW) dựa trên lý do tránh được phép băm liên tục. Bài báo này phân tích bảo mật đồng thuận từ góc độ cân bằng dựa trên kỳ vọng và chỉ ra rằng đối với bất kỳ hệ thống không cần cấp phép nào cung cấp phần thưởng khối có giá trị bên ngoài, những kẻ tấn công và người bảo vệ hợp lý đều có động cơ chi tiêu tài nguyên thực tế tỷ lệ với giá trị kỳ vọng đang bị rủi ro. Bằng Chứng Công Việc thể hiện khoản chi tiêu này một cách trực tiếp và minh bạch thông qua mức tiêu thụ năng lượng, trong khi Bằng Chứng Cổ Phần chuyển dịch nó sang các kênh không đồng nhất và mờ đục như nhân bản cơ sở hạ tầng, sự gia tăng danh tính trình xác nhận, tối ưu hóa do MEV thúc đẩy, chiếm đoạt quản trị và chi phí tổ chức. Chúng tôi tiếp tục chỉ ra rằng PoW duy nhất cung cấp một thước đo chi tiêu bảo mật trên mỗi đơn vị phát hành có thể nhìn thấy ở cấp giao thức, cho phép suy luận thuật toán về chính sách tiền tệ mà không cần dựa vào các tiên tri xã hội hay tổ chức. Những kết quả này bác bỏ tuyên bố rằng PoS loại bỏ chi phí năng lượng ở trạng thái cân bằng và xác lập PoW như một nền tảng bản thể luận riêng biệt cho bảo mật được tiết lộ đối nghịch và có thể đọc được.

1 Giới Thiệu

Những chỉ trích về môi trường đối với Bằng Chứng Công Việc đã thúc đẩy việc áp dụng rộng rãi các cơ chế đồng thuận Bằng Chứng Cổ Phần. Luận điểm thống trị khẳng định rằng PoS đạt được bảo mật tương đương với mức tiêu thụ năng lượng thấp hơn đáng kể, vì các trình xác nhận chỉ cần thực hiện tính toán nhẹ.

Bài báo này lập luận rằng những so sánh như vậy dựa trên một lỗi phân loại. Trong bất kỳ hệ thống đồng thuận không cần cấp phép nào cung cấp phần thưởng khối được định giá bên ngoài, chi tiêu bảo mật cân bằng được neo đậu vào giá trị kỳ vọng của phần thưởng đó. Những kẻ tấn công hợp lý sẽ chi tiêu tài nguyên lên đến lợi ích kỳ vọng từ cuộc tấn công, và những người bảo vệ hợp lý phải chi tiêu tài nguyên tương đương để ngăn chặn việc chiếm đoạt. Đây là ứng dụng trực tiếp của tiêu tán thuê cạnh tranh [**?**, **?**], được Budish áp dụng gần đây nhất vào đồng thuận blockchain [**?**]. Thay đổi cơ chế đồng thuận chỉ thay đổi *hình thức* và *khả năng hiển thị* của chi tiêu, không phải sự tồn tại của nó.

Chúng tôi chỉ ra rằng Bằng Chứng Công Việc duy nhất làm cho chi tiêu bảo mật có thể đọc được đối với chính giao thức, trong khi Bằng Chứng Cổ Phần chuyển dịch chi tiêu tương đương sang các hình thức tổ chức ít đo lường được và thường kém hiệu quả hơn. Sự phân biệt này có ý nghĩa không chỉ đối với kế toán năng lượng, mà còn đối với thiết kế tiền tệ.

2 Phần Thưởng Khối và Chi Tiêu Bảo Mật Cân Bằng

Cho thời gian được lập chỉ mục theo chiều cao khối t. Định nghĩa:

- P_t: giá bên ngoài của tài sản gốc (ví dụ: USD/đồng xu),
- R_t: lượng phát hành (đồng xu/khối),
- F_t: phí giao dịch (đồng xu/khối),
- M_t: giá trị có thể trích xuất thêm (đồng xu/khối).

Định nghĩa tổng phần thưởng khối tính bằng đồng xu:

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

và giá trị bên ngoài của nó:

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

Tất cả các đại lượng đều có thể ngẫu nhiên; do đó chúng tôi suy luận theo kỳ vọng.

2.1 Động cơ tấn công

Kẻ tấn công có động cơ tấn công khi và chỉ khi:

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

trong đó G_t là lợi ích bên ngoài từ cuộc tấn công và C_t^{att} là chi phí bên ngoài phát sinh.

Trong môi trường mở, cạnh tranh, các cơ hội kéo dài để chiếm đoạt V_t với chi phí thấp hơn nhiều so với V_t sẽ bị loại bỏ. Do đó, chi tiêu của kẻ tấn công ở trạng thái cân bằng thỏa mãn:

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

với $\alpha \in (0, 1]$, và $\alpha > 1$ có thể xảy ra khi các cuộc tấn công mở khóa các khoản thanh toán bên ngoài bổ sung.

2.2 Động cơ phòng thủ

Để ngăn chặn tấn công, những người bảo vệ phải tăng chi phí của kẻ tấn công hoặc khớp với năng lực của kẻ tấn công. Trong cả hai trường hợp:

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

Do đó chi tiêu bảo mật cân bằng bị giới hạn dưới bởi giá trị kỳ vọng đang bị rủi ro, bất kể cơ chế đồng thuận.

3 Chi Phí Bên Ngoài như một Tiên Đề Bảo Mật

Sách trắng Bitcoin gốc ngầm dựa vào nguyên tắc rằng bảo mật bền vững đòi hỏi chi tiêu bên ngoài không thể thu hồi [**?**]. Chúng tôi nâng giả định này lên thành một tiên đề rõ ràng.

Tiên Đề (Chi Phí Bên Ngoài của Kiểm Soát). *Trong một hệ thống đồng thuận không cần cấp phép, kiểm soát bền vững các chuyển đổi trạng thái đòi hỏi chi tiêu không thể đảo ngược trong một nền tảng được định giá bên ngoài hệ thống.*

Tiên đề này không chỉ định nền tảng cụ thể, chỉ yêu cầu nó phải là bên ngoài, tốn kém và không thể thu hồi.

4 Nguyên Lý Hiện Thân

Nguyên Lý (Hiện Thân Nền Tảng). *Bất kỳ chi tiêu chiến lược nào trong một trò chơi thực tế đều phải được khởi tạo trong một nền tảng bản thể luận, và do đó kéo theo mức tiêu thụ tài nguyên và năng lượng khác không đặc trưng cho nền tảng đó.*

Chi tiêu cho phần cứng, lao động, tòa nhà, phối hợp, quản trị và thực thi đều kéo theo năng lượng hiện thân thông qua sản xuất và vận hành. Sử dụng năng lượng có thể trực tiếp hoặc gián tiếp, nhưng không thể loại bỏ nếu chi phí bên ngoài là bắt buộc.

Nguyên lý này thiết lập rằng chi tiêu bảo mật PoS là khác không nhưng bản thân nó không thiết lập độ lớn. So sánh liên quan không phải là về sự tồn tại mà là về quy mô: liệu chi tiêu PoS bị chuyển dịch có tiệm cận chi tiêu PoW ở các mức bảo mật tương đương không? Điều này phụ thuộc vào các kênh nào hấp thụ chi tiêu bị chuyển dịch và cường độ năng lượng của chúng so với phép băm trực tiếp. Mục **??** phát triển luận điểm rằng các kênh liên quan—cơ sở hạ tầng MEV, dự phòng trình xác nhận, phối hợp quản trị—được hiện thân về mặt năng lượng ở quy mô có thể so sánh với chi tiêu khai thác trực tiếp ở các mức bảo mật tương đương.

5 Bằng Chứng Công Việc và Chi Tiêu Bảo Mật Có Thể Đọc Được

Trong các hệ thống Bằng Chứng Công Việc, chi tiêu bảo mật được thể hiện trực tiếp thông qua mức tiêu thụ năng lượng.

Cho:

- $\mathcal{H}_t$: số lần băm kỳ vọng cần thiết mỗi khối (hàm của độ khó),
- e_t: joule mỗi lần băm,
- c_t: giá điện (USD/joule).

Chi phí điện kỳ vọng mỗi khối là:

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

Đối với cuộc tấn công yêu cầu kiểm soát trong k khối, việc ngăn chặn đòi hỏi:

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

Sắp xếp lại thu được giới hạn giá ngầm định:

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

5.1 Mật độ bảo mật có thể nhìn thấy ở cấp giao thức

Quan trọng là, các giao thức PoW quan sát $\mathcal{H}_t$ và Π_t trực tiếp. Do đó, trình nền có thể tính toán:

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

công việc không thể đảo ngược kỳ vọng hỗ trợ mỗi đơn vị phát hành.

Điều này cung cấp một thước đo trực tiếp, được tiết lộ đối nghịch, gốc giao thức về chi tiêu bảo mật mỗi đồng xu. Không có đại lượng tương đương nào tồn tại trong các hệ thống Bằng Chứng Cổ Phần.

Các tính chất lý thuyết trò chơi của σ_t như một tín hiệu đáng được chú ý. Hai câu hỏi nổi lên. Thứ nhất, σ_t có thể bị các thợ đào lớn thao túng không? Vì $\mathcal{H}_t$ được xác định bởi độ khó (trung bình trễ trên nhiều khối), thao túng ngắn hạn có tác động hạn chế; việc trình bày sai bền vững đòi hỏi từ bỏ phần thưởng khối ở tốc độ vượt quá lợi nhuận thao túng đối với bất kỳ $\mu < 1/2$ nào. Thứ hai, các động lực cân bằng là gì nếu chính sách tiền tệ phản hồi với σ_t? Nếu lượng phát hành điều chỉnh theo σ_t, các thợ đào dự đoán điều này và điều chỉnh tỷ lệ băm theo đó—một phản ứng chiến lược mà cơ chế tiền tệ thích nghi phải tính đến. Những động lực này được phân tích trong [**?**].

Nhận xét (Tín hiệu Trễ). Vì độ khó được tính toán như một trung bình luân phiên trên nhiều khối (2016 khối trong Bitcoin), σ_t phản ánh chi tiêu bảo mật lịch sử hơn là tức thời. Sự sụp đổ nhanh chóng về tỷ lệ băm—ví dụ, việc đóng cửa theo quy định của một khu vực khai thác lớn—khiến σ_t cao một cách giả tạo trong toàn bộ cửa sổ điều chỉnh độ khó trước khi thuật toán độ khó điều chỉnh. Các hệ thống sử dụng σ_t như một tín hiệu thích nghi phải tính đến độ trễ này, thông qua các tham số phản hồi thận trọng hoặc bằng cách theo dõi các tín hiệu thời gian thực phụ trợ như phương sai khoảng cách khối quan sát được.

6 Chi Tiêu Bị Chuyển Dịch trong Bằng Chứng Cổ Phần

Bằng Chứng Cổ Phần loại bỏ phép băm liên tục nhưng không loại bỏ động cơ chi tiêu tài nguyên lên đến $\mathbb{E}[V_t]$. Thay vào đó, chi tiêu bị chuyển dịch sang nhiều kênh:

- sự gia tăng danh tính trình xác nhận và nhân bản cơ sở hạ tầng,

- tối ưu hóa do MEV thúc đẩy, cuộc đua độ trễ và phần cứng chuyên dụng,
- chiếm đoạt quản trị, phối hợp và thực thi,
- chi phí tổ chức về lưu ký, pháp lý và tuân thủ.

Cho C_t^{pos} ký hiệu tổng chi phí bên ngoài trên tất cả các kênh đó. Bảo mật cân bằng đòi hỏi:

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

Những chi phí này vẫn được hiện thân về mặt năng lượng nhưng không thể đọc được ở cấp giao thức và khó để kiểm toán hay tối ưu hóa.

Nhận xét (Bất Đối Xứng Mô Hình Mối Đe Dọa). So sánh chi tiêu ở trên giả định các cuộc tấn công hướng đến cùng một mục tiêu: kiểm soát một phần đủ của việc tham gia đồng thuận tích cực để viết lại lịch sử gần đây. Tuy nhiên, PoW và PoS đối mặt với các vectơ tấn công khác nhau về mặt phân loại. Các hệ thống PoS còn dễ bị tổn thương với *các cuộc tấn công tầm xa*: đối thủ chiếm được khóa riêng của trình xác nhận cũ (từ những người tham gia sớm, sàn giao dịch bị xâm phạm, hoặc các khoản tiền đặt cọc có thể bị phạt đã được rút) có thể viết lại lịch sử từ kỷ nguyên trước đó với chi phí không đáng kể, vì các khóa đó không còn phơi bày kinh tế liên tục. Cuộc tấn công này cực kỳ tốn kém trong PoW—viết lại các khối đòi hỏi phải chi tiêu lại năng lượng cho mọi khối trong chuỗi bị viết lại, một ràng buộc vật lý không thể rút gọn. Khung tiêu tán thuê đặc trưng cho chi tiêu cân bằng cho việc tham gia liên tục; nó không nắm bắt được chi phí bất đối xứng của lớp tấn công khác biệt về chất này. Các hệ thống PoS giải quyết điều này thông qua các điểm kiểm tra tính chủ quan yếu hoặc đồng thuận xã hội về tính chung cuộc, tái giới thiệu sự phối hợp tổ chức mà mô hình tiêu tán thuê không yêu cầu.

7 Phát Hành, Thông Lượng và Các Ràng Buộc Bị Quy Nhầm

Một quan niệm sai lầm phổ biến là Bằng Chứng Công Việc vốn dĩ giới hạn thông lượng giao dịch. Điều này nhầm lẫn đồng thuận với lập kế hoạch năng lực. PoW xác định việc lựa chọn lãnh đạo và chi phí bảo mật; thông lượng được xác định bởi kích thước khối, tần suất khối và thiết kế mạng.

Các giới hạn thông lượng quan sát được trong Bitcoin phát sinh từ các lựa chọn tham số rõ ràng và quyết định quản trị, không phải từ chính Bằng Chứng Công Việc.

8 Phát Hành do Con Người Kiểm Soát và Thất Bại Chiến Lược

Bất kỳ cơ chế phát hành nào phụ thuộc vào quyền quyết định của con người đều giới thiệu các động cơ trò chơi lặp lại, thông tin bất cân xứng và chiếm đoạt chiến lược. Theo thời gian, các hệ thống như vậy thể hiện sự xói mòn độ tín nhiệm và phát hành quá mức.

Ngược lại, PoW phơi bày một tín hiệu chi tiêu bảo mật được tạo ra đối nghịch, phi xã hội. Các cơ chế phát hành phản hồi thuật toán với tín hiệu này tránh kiểm soát tùy ý và các tiên tri tổ chức.

9 Kết Luận

Chúng tôi đã chỉ ra rằng chi tiêu bảo mật cân bằng trong đồng thuận không cần cấp phép được neo đậu vào giá trị bên ngoài kỳ vọng đang bị rủi ro. Bằng Chứng Công Việc thể hiện khoản chi tiêu này một cách trực tiếp và minh bạch thông qua mức tiêu thụ năng lượng và duy nhất cung cấp một thước đo chi tiêu bảo mật trên mỗi đơn vị phát hành có thể nhìn thấy ở cấp giao thức. Bằng Chứng Cổ Phần không loại bỏ chi phí năng lượng ở trạng thái cân bằng; nó chuyển dịch chúng sang các hình thức tổ chức mờ đục và thường kém hiệu quả hơn.

Những kết quả này bác bỏ các tuyên bố rằng PoS vốn dĩ ưu việt về môi trường và xác lập PoW như một nền tảng bản thể luận riêng biệt cho bảo mật được tiết lộ đối nghịch và có thể đọc được. Các hàm ý cho thiết kế tiền tệ và phát hành thích nghi được phát triển trong [**?**], nơi chỉ định một cơ chế hai vòng không cần tiên tri sử dụng proxy công việc σ_t như một tín hiệu phát hành thích nghi. Việc khởi tạo cấp giao thức của đốt-để-nói (burn-to-speak) như một lớp nhắn tin liên kết chống thư rác được chỉ định trong [**?**].

Tài liệu

[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. Bản in trước, 2026.

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