الإنفاق الأمني والطاقة وإمكانية قراءة الإصدار في آليات الإجماع غير المرخّصة

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

٢١ فبراير ٢٠٢٦
1.1 Version

ملخص

كثيرًا ما تُوصف أنظمة إثبات الحصة (PoS) بأنها بدائل صديقة للبيئة لأنظمة إثبات العمل (PoW)، استنادًا إلى أنها تتجنب عمليات التجزئة المستمرة. تحلل هذه الورقة أمن الإجماع من منظور التوازن القائم على التوقعات، وتُثبت أنه في أي نظام غير مرخّص يقدم مكافأة كتلة ذات قيمة خارجية، يُحفَّز المهاجمون والمدافعون العقلانيون على إنفاق موارد حقيقية تتناسب مع القيمة المتوقعة للأصول المعرضة للخطر. يُعبّر إثبات العمل عن هذا الإنفاق بصورة مباشرة وقابلة للقراءة من خلال استهلاك الطاقة، في حين يُحوّله إثبات الحصة إلى قنوات متباينة وغير شفافة، كتكرار البنية التحتية، وتكاثر هويات المدققين، والتحسين المدفوع بالقيمة القابلة للاستخراج من المعدّنين (MEV)، والاستيلاء على الحوكمة، والتكاليف المؤسسية. نُثبت كذلك أن PoW يوفر بصورة فريدة مقياسًا مرئيًا على مستوى البروتوكول للإنفاق الأمني لكل وحدة إصدار، مما يتيح الاستدلال الخوارزمي على السياسة النقدية دون الحاجة إلى أوراكلات اجتماعية أو مؤسسية. تُقوّض هذه النتائج الادعاء بأن PoS يُلغي تكاليف الطاقة في حالة التوازن، وتُرسّخ PoW بوصفه ركيزة وجودية متميزة لأمن قابل للقراءة ومكشوف بصورة تعارضية.

١ مقدمة

أفضت الانتقادات البيئية الموجهة إلى إثبات العمل إلى انتشار واسع لآليات إجماع إثبات الحصة. تزعم الرواية السائدة أن PoS يحقق أمانًا مماثلًا مع استهلاك أدنى بكثير للطاقة، إذ لا يحتاج المدققون إلا إلى إجراء عمليات حسابية خفيفة.

تُجادل هذه الورقة بأن هذه المقارنات تقوم على خطأ في التصنيف. في أي نظام إجماع غير مرخّص يقدم مكافأة كتلة مُسعَّرة خارجيًا، يرتبط الإنفاق الأمني في حالة التوازن بالقيمة المتوقعة لتلك المكافأة. سيُنفق الخصوم العقلانيون الموارد حتى الحد الذي يساوي فيه العائد المتوقع من الهجوم، ويجب على المدافعين العقلانيين إنفاق موارد مماثلة لردع الاستيلاء. وهذا تطبيق مباشر لنظرية التبديد التنافسي للريع [1, 2]، وقد طبّقها مؤخرًا Budish على إجماع سلسلة الكتل [3]. إن تغيير آلية الإجماع يُغيّر شكل الإنفاق ومدى رؤيته، لا وجوده.

نُثبت أن إثبات العمل يجعل الإنفاق الأمني مقروءًا للبروتوكول نفسه بصورة فريدة، في حين يُحوّل إثبات الحصة الإنفاق المعادل إلى أشكال مؤسسية أقل قابلية للقياس وأدنى كفاءة في الغالب. لهذا التمييز انعكاسات لا على محاسبة الطاقة وحسب، بل على تصميم العملة أيضًا.

٢ مكافآت الكتل والإنفاق الأمني في حالة التوازن

ليكن الزمن مفهرسًا بارتفاع الكتلة t. نُعرِّف:

- P_t: السعر الخارجي للأصل الأصلي (مثلًا دولار أمريكي لكل عملة)،

- R_t: الإصدار (عملات/كتلة)،
- F_t: رسوم المعاملات (عملات/كتلة)،
- M_t: القيمة الإضافية القابلة للاستخراج (عملات/كتلة).

نُعرِّف إجمالي مكافأة الكتلة بالعملة:

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

وقيمتها الخارجية:

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

جميع الكميات عشوائية محتملة؛ لذا نستدل في إطار التوقع.

١.٢ حوافز الهجوم

يُحفَّز المهاجم على الهجوم حين يتحقق:

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

حيث G_t هو العائد الخارجي من الهجوم، وC_t^{att} هو التكلفة الخارجية المتحمَّلة.

في البيئات ذات الدخول المفتوح والتنافسية، تُقضى الفرص المستدامة لالتقاط V_t بتكلفة أدنى بكثير من V_t. وبالتالي، يُحقق إنفاق المهاجم في حالة التوازن:

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

لبعض $\alpha \in (0, 1]$، مع إمكانية تحقق $\alpha > 1$ حين تُفتح الهجمات عوائد خارجية إضافية.

٢.٢ حوافز الدفاع

لردع الهجوم، يجب على المدافعين رفع تكاليف المهاجم أو مجاراة قدرته. في كلتا الحالتين:

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

وبذلك يكون الإنفاق الأمني في حالة التوازن مقيَّدًا من الأسفل بالقيمة المتوقعة للأصول المعرضة للخطر، بصرف النظر عن آلية الإجماع.

٣ التكلفة الخارجية كمسلّمة أمنية

يعتمد ورقة بيتكوين البيضاء الأصلية ضمنيًا على مبدأ مفاده أن الأمن الدائم يستلزم إنفاقًا خارجيًا غير قابل للاسترداد [4]. نرفع هذا الافتراض إلى مسلّمة صريحة.

مسلّمة (التكلفة الخارجية للسيطرة). في نظام إجماع غير مرخّص، تستلزم السيطرة الدائمة على انتقالات الحالة إنفاقًا لا رجعة فيه في ركيزة مُسعَّرة خارجيًا عن النظام ذاته.

لا تُحدد هذه المسلّمة طبيعة الركيزة، بل تشترط فقط أن تكون خارجية ومُكلفة وغير قابلة للاسترداد.

٤ مبدأ التجسيد

مبدأ (تجسيد الركيزة). يجب أن يتجسد أي إنفاق استراتيجي في لعبة بالعالم الحقيقي في ركيزة وجودية، وبالتالي يستلزم استهلاكًا غير صفري من الموارد والطاقة خاصًا بتلك الركيزة.

يستلزم الإنفاق على الأجهزة والعمالة والمباني والتنسيق والحوكمة والإنفاذ طاقةً متجسدة من خلال الإنتاج والتشغيل. قد يكون استخدام الطاقة مباشرًا أو غير مباشر، لكن لا يمكن إلغاؤه إذا اشترطنا تكلفة خارجية.

يُثبت هذا المبدأ أن الإنفاق الأمني في PoS غير صفري، لكنه لا يُحدد حجمه بذاته. المقارنة الجوهرية ليست في الوجود بل في الحجم: هل يقترب الإنفاق المُحوَّل في PoS من إنفاق PoW لمستويات أمان مكافئة؟ يعتمد ذلك على القنوات التي تستوعب الإنفاق المُحوَّل وعلى كثافتها الطاقوية نسبةً إلى التجزئة المباشرة. يُطور القسم ٦ الادعاءَ بأن القنوات ذات الصلة---بنية تحتية MEV، وتكرار المدققين، وتنسيق الحوكمة---متجسدة طاقويًا بحجم مقارن لإنفاق التعدين المباشر لمستويات أمان مكافئة.

٥ إثبات العمل والإنفاق الأمني المقروء

في أنظمة إثبات العمل، يُعبَّر عن الإنفاق الأمني مباشرةً من خلال استهلاك الطاقة.
ليكن:

- $\mathcal{H}_t$: عدد التجزئات المتوقعة المطلوبة لكل كتلة (دالة الصعوبة)،
- e_t: الجول لكل تجزئة،
- c_t: سعر الكهرباء (دولار/جول).

التكلفة الكهربائية المتوقعة لكل كتلة:

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

لهجوم يستلزم التحكم في k كتلة، يتطلب الردع:

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

بإعادة الترتيب نحصل على حد أعلى ضمني للسعر:

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

١.٥ كثافة الأمن المرئية على مستوى البروتوكول

الأمر الجوهري أن بروتوكولات PoW ترصد $\mathcal{H}_t$ وΠ_t مباشرةً. لذا يمكن للعفريت حساب:

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

وهو العمل الذي لا رجعة فيه المتوقع الداعم لكل وحدة إصدار.

يوفر هذا مقياسًا حيًا ومكشوفًا بصورة تعارضية وأصيلًا للبروتوكول للإنفاق الأمني لكل عملة. لا يوجد ما يعادل هذه الكمية في أنظمة إثبات الحصة.

تستحق الخصائص النظرية للألعاب لـσ_t بوصفه إشارةً الاهتمامَ. تبرز هنا مسألتان. أولًا، هل يمكن للمعدّنين الكبار التلاعب بـσ_t؟ بما أن $\mathcal{H}_t$ يُحدَّد بالصعوبة (متوسط متأخر على كتل كثيرة)، فإن التلاعب قصير الأمد له أثر محدود، ويستلزم التمثيل الكاذب

المستدام التخلي عن مكافآت الكتل بمعدل يتجاوز مكسب التلاعب لأي $\mu < 1/2$. ثانيًا، ما ديناميكيات التوازن إذا استجابت السياسة النقدية لـσ_t؟ إذا تعدّل الإصدار استجابةً لـσ_t، يتوقع المعدّنون ذلك ويعدّلون معدل التجزئة تبعًا له---وهي استجابة استراتيجية ينبغي لآلية العملة التكيفية أخذها بعين الاعتبار. تُحلَّل هذه الديناميكيات في [5].

ملاحظة (الإشارة المتأخرة). بما أن الصعوبة تُحسب كمتوسط متحرك على كتل كثيرة (2016 كتلة في بيتكوين)، يعكس σ_t الإنفاق الأمني التاريخي لا اللحظي. قد يؤدي الانهيار المفاجئ في طاقة التجزئة---كإغلاق تنظيمي لمنطقة تعدين مهيمنة---إلى بقاء σ_t مرتفعًا اصطناعيًا طوال نافذة تعديل الصعوبة بأكملها قبل أن تتصحح. يجب على الأنظمة التي تستخدم σ_t كإشارة تكيفية مراعاة هذا التأخر، إما من خلال معامل استجابة محافظ أو بمراقبة إشارات مساعدة في الوقت الفعلي كتباين الفترة الزمنية المرصودة بين الكتل.

٦ الإنفاق المُحوَّل في إثبات الحصة

يُلغي إثبات الحصة التجزئة المستمرة لكنه لا يُلغي الحافز على إنفاق الموارد حتى $\mathbb{E}[V_t]$. عوضًا عن ذلك، يُحوَّل الإنفاق إلى قنوات متعددة:

- تكاثر هويات المدققين وتكرار البنية التحتية،
- التحسين المدفوع بـMEV، وسباقات الزمن، والأجهزة المتخصصة،
- الاستيلاء على الحوكمة والتنسيق والإنفاذ،
- التكاليف الحضانية والقانونية والامتثالية.

ليكن C_t^{pos} يُمثّل إجمالي التكلفة الخارجية عبر جميع هذه القنوات. يستلزم الأمن في حالة التوازن:

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

تبقى هذه التكاليف متجسدة طاقويًا لكنها ليست مقروءة من البروتوكول ويصعب تدقيقها أو تحسينها.

ملاحظة (عدم تماثل نموذج التهديد). يفترض مقارنة الإنفاق أعلاه أن الهجمات تستهدف الهدف ذاته: السيطرة على حصة كافية من مشاركة الإجماع النشطة لإعادة كتابة التاريخ الأخير. غير أن PoW وPoS يواجهان ناقلات هجوم مختلفة اختلافًا جذريًا. تكون أنظمة PoS عرضةً إضافيًا لـالهجمات بعيدة المدى: قد يحصل المهاجم الذي يحوز مفاتيح خاصة قديمة للمدققين (من مشاركين مبكرين أو بورصات مخترقة أو ودائع قابلة للشطب سُحبت لاحقًا) على إعادة كتابة التاريخ من حقبة سابقة بتكلفة ضئيلة، إذ لا تنطوي تلك المفاتيح على تعرض اقتصادي مستمر. هذا الهجوم باهظ التكلفة في PoW---إذ تستلزم إعادة كتابة الكتل إعادة إنفاق الطاقة لكل كتلة في السلسلة المُعاد كتابتها، وهو قيد فيزيائي لا يمكن اختزاله. يُصوّر إطار تبديد الريع الإنفاق التوازني للمشاركة المستمرة؛ وهو لا يلتقط التكلفة غير المتماثلة لهذه الفئة المتميزة من الهجمات. تعالج أنظمة PoS هذا من خلال نقاط تفتيش الذاتية الضعيفة أو الإجماع الاجتماعي على النهائية، مما يُعيد إدخال التنسيق المؤسسي الذي لم يكن نموذج تبديد الريع يستلزمه.

٧ الإصدار والإنتاجية والقيود المنسوبة خطأً

من المفاهيم الخاطئة الشائعة أن إثبات العمل يُقيّد بطبيعته إنتاجية المعاملات. هذا الرأي يخلط بين الإجماع وتخطيط الطاقة الاستيعابية. يُحدد PoW اختيار القائد وتكلفة الأمن؛ أما الإنتاجية فيُحددها حجم الكتلة وتكرار الكتل وتصميم الشبكة.

تنشأ قيود الإنتاجية المرصودة في بيتكوين من خيارات معاملات واضحة وقرارات حوكمة، لا من إثبات العمل ذاته.

٨ الإصدار تحت السيطرة البشرية والإخفاق الاستراتيجي

أي آلية إصدار تعتمد على السلطة التقديرية البشرية تُدخل حوافز اللعبة المتكررة، وعدم تماثل المعلومات، والاستيلاء الاستراتيجي. بمرور الوقت، تُظهر مثل هذه الأنظمة تآكل المصداقية والإصدار المفرط.

في المقابل، يكشف PoW عن إشارة للإنفاق الأمني مولَّدة بصورة تعارضية وغير اجتماعية. تتجنب آليات الإصدار التي تستجيب خوارزميًا لهذه الإشارة السيطرة التقديرية والأوراكلات المؤسسية.

٩ خاتمة

أثبتنا أن الإنفاق الأمني في حالة التوازن في الإجماع غير المرخّص مرتبط بالقيمة الخارجية المتوقعة للأصول المعرضة للخطر. يُعبّر إثبات العمل عن هذا الإنفاق بصورة مباشرة وقابلة للقراءة من خلال استهلاك الطاقة، ويوفر بصورة فريدة مقياسًا مرئيًا على مستوى البروتوكول للإنفاق الأمني لكل وحدة إصدار. لا يُلغي إثبات الحصة تكاليف الطاقة في حالة التوازن، بل يُحوّلها إلى أشكال مؤسسية غير شفافة وأقل كفاءة في الغالب.

تُقوّض هذه النتائج الادعاءات بأن PoS أفضل بيئيًا بطبيعته، وتُرسّخ PoW بوصفه ركيزة وجودية متميزة لأمن قابل للقراءة ومكشوف بصورة تعارضية. الانعكاسات على تصميم العملة والإصدار التكيفي مُطوَّرة في [5]، الذي يُحدد آلية حلقة مزدوجة خالية من الأوراكلات تستخدم الوكيل للعمل σ_t كإشارة إصدار تكيفية. يُحدَّد التجسيد على مستوى البروتوكول للحرق مقابل الكلام (burn-to-speak) بوصفه طبقة رسائل فيدرالية مضادة للبريد العشوائي في [6].

المراجع

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

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

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

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

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

[٦] Chancellor, S. CashWeb: A Cryptocurrency-Integrated Protocol for Federated Anti-Spam Messaging, Preprint, 2026.