अनुमति-रहित सर्वसम्मति में सुरक्षा व्यय, ऊर्जा और निर्गमन सुपाठ्यता

□□□□□□□ □□□□□□□□□□
shammah.chancellor@proton.me
https://t.me/TheLotusNetwork

२१ फ़रवरी २०२६
□□□□□□□ 1.1

सारांश

प्रूफ-ऑफ-स्टेक (□□□) प्रणालियों को सामान्यतः प्रूफ-ऑफ-वर्क (□□□) के पर्यावरण-अनुकूल विकल्प के रूप में वर्णित किया जाता है, इस आधार पर कि वे निरंतर हैशिंग से बचती हैं। यह शोधपत्र एक संतुलन, प्रत्याशा-आधारित दृष्टिकोण से सर्वसम्मति सुरक्षा का विश्लेषण करता है और दर्शाता है कि किसी भी अनुमति-रहित प्रणाली के लिए जो बाह्य रूप से मूल्यवान ब्लॉक पुरस्कार प्रदान करती है, तर्कसंगत आक्रमणकर्ता और रक्षक दोनों ही जोखिम में पड़े अपेक्षित मूल्य के अनुपात में वास्तविक संसाधन व्यय करने के लिए प्रोत्साहित होते हैं। प्रूफ-ऑफ-वर्क इस व्यय को ऊर्जा खपत के माध्यम से प्रत्यक्ष और सुपाठ्य रूप से व्यक्त करता है, जबकि प्रूफ-ऑफ-स्टेक इसे विषम और अपारदर्शी चैनलों जैसे अवसंरचना दोहराव, सत्यापनकर्ता पहचान प्रसार, □□□-संचालित अनुकूलन, शासन अधिग्रहण और संस्थागत ऊपरी व्यय में विस्थापित करता है। हम आगे दर्शाते हैं कि □□□ विशिष्ट रूप से प्रति निर्गमन इकाई सुरक्षा व्यय का एक प्रोटोकॉल-दृश्य माप प्रदान करता है, जो सामाजिक या संस्थागत ओरेकल पर निर्भरता के बिना मौद्रिक नीति के बारे में एल्गोरिदमिक तर्क को सक्षम बनाता है। ये परिणाम इस दावे को कमज़ोर करते हैं कि □□□ संतुलन में ऊर्जा लागतों को समाप्त करता है और □□□ को सुपाठ्य, प्रतिकूल-प्रकट सुरक्षा के लिए एक विशिष्ट ऑन्टोलॉजिकल सब्सट्रेट के रूप में स्थापित करते हैं।

1 परिचय

प्रूफ-ऑफ-वर्क की पर्यावरणीय आलोचनाओं ने प्रूफ-ऑफ-स्टेक सर्वसम्मति तंत्रों को व्यापक रूप से अपनाने में योगदान दिया है। प्रमुख आख्यान यह दावा करता है कि □□□ काफी कम ऊर्जा खपत के साथ तुलनीय सुरक्षा प्राप्त करता है, क्योंकि सत्यापनकर्ताओं को केवल हल्की गणना करनी होती है।

यह शोधपत्र तर्क देता है कि ऐसी तुलनाएं एक श्रेणी-संबंधी भूल पर आधारित हैं। किसी भी अनुमति-रहित सर्वसम्मति प्रणाली में जो बाह्य रूप से मूल्य-निर्धारित ब्लॉक पुरस्कार प्रदान करती है, संतुलन सुरक्षा व्यय उस पुरस्कार के अपेक्षित मूल्य से आबद्ध होता है। तर्कसंगत विरोधी आक्रमण से अपेक्षित लाभ तक संसाधन व्यय करेंगे, और तर्कसंगत रक्षकों को अधिग्रहण को रोकने के लिए तुलनीय संसाधन व्यय करने होंगे। यह प्रतिस्पर्धी किराया विसर्जन का एक प्रत्यक्ष अनुप्रयोग है [?, ?], जिसे हाल ही में □□□□□□ ने ब्लॉकचेन सर्वसम्मति पर लागू किया है [?]। सर्वसम्मति तंत्र को बदलने से व्यय का स्वरूप और दृश्यता बदलती है, न कि उसका अस्तित्व।

हम दर्शाते हैं कि प्रूफ-ऑफ-वर्क विशिष्ट रूप से सुरक्षा व्यय को प्रोटोकॉल के लिए सुपाठ्य बनाता है, जबकि प्रूफ-ऑफ-स्टेक समतुल्य व्यय को कम मापनीय और अक्सर कम कुशल संस्थागत रूपों में विस्थापित करता है। यह अंतर न केवल ऊर्जा लेखांकन के लिए, बल्कि मौद्रिक डिज़ाइन के लिए भी निहितार्थ रखता है।

2 ब्लॉक पुरस्कार और संतुलन सुरक्षा व्यय

माना कि समय को ब्लॉक ऊंचाई t द्वारा अनुक्रमित किया गया है। परिभाषित करें:

- P_t: मूल संपत्ति का बाह्य मूल्य (उदा. □□□/सिक्का),
- R_t: निर्गमन (सिक्के/ब्लॉक),
- F_t: लेनदेन शुल्क (सिक्के/ब्लॉक),
- M_t: अतिरिक्त निकाली जा सकने वाली मूल्य (सिक्के/ब्लॉक)।

सिक्कों में कुल ब्लॉक पुरस्कार परिभाषित करें:

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

और इसका बाह्य मूल्य:

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

सभी राशियाँ संभावित रूप से स्टोकास्टिक हैं; इसलिए हम प्रत्याशा में तर्क करते हैं।

2.1 आक्रमण प्रोत्साहन

एक आक्रमणकर्ता तब आक्रमण करने के लिए प्रोत्साहित होता है जब:

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

जहाँ G_t आक्रमण से बाह्य लाभ है और $C_t^{\square\square\square}$ वहन की गई बाह्य लागत है।

खुले-प्रवेश, प्रतिस्पर्धी वातावरण में, V_t से बहुत कम लागत पर V_t को लगातार अधिग्रहित करने के अवसर समाप्त हो जाते हैं। फलतः, संतुलन आक्रमणकर्ता व्यय संतुष्ट करता है:

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

किसी $\alpha \in (0, 1]$ के लिए, जब आक्रमण अतिरिक्त बाह्य भुगतान अनलॉक करते हैं तो $\alpha > 1$ संभव है।

2.2 रक्षा प्रोत्साहन

आक्रमण को रोकने के लिए, रक्षकों को आक्रमणकर्ता की लागत बढ़ानी होगी या आक्रमणकर्ता की क्षमता से मेल खाना होगा। किसी भी स्थिति में:

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

इस प्रकार संतुलन सुरक्षा व्यय जोखिम में पड़े अपेक्षित मूल्य द्वारा निम्न-आबद्ध है, सर्वसम्मति तंत्र से स्वतंत्र रूप से।

3 बाह्य लागत एक सुरक्षा अभिगृहीत के रूप में

मूल □□□□□□□ श्वेतपत्र अंतर्निहित रूप से इस सिद्धांत पर निर्भर करता है कि स्थायी सुरक्षा के लिए अपुनः प्राप्य बाह्य व्यय की आवश्यकता होती है [?]। हम इस मान्यता को एक स्पष्ट अभिगृहीत के रूप में उन्नत करते हैं।

अभिगृहीत (नियंत्रण की बाह्य लागत). एक अनुमति-रहित सर्वसम्मति प्रणाली में, अवस्था-संक्रमणों पर स्थायी नियंत्रण के लिए स्वयं प्रणाली के बाहर मूल्य-निर्धारित सब्सट्रेट में अपरिवर्तनीय व्यय की आवश्यकता होती है।

यह अभिगृहीत सब्सट्रेट को निर्दिष्ट नहीं करता, केवल यह कि वह बाह्य, व्ययपूर्ण और अपुनः प्राप्य हो।

4 अवतरण सिद्धांत

सिद्धांत (सब्सट्रेट अवतरण). एक वास्तविक-विश्व खेल में किसी भी रणनीतिक व्यय को एक ऑन्टोलॉजिकल सब्सट्रेट में तात्कालिक किया जाना चाहिए, और इसलिए उस सब्सट्रेट के लिए विशिष्ट गैर-शून्य संसाधन और ऊर्जा खपत को अनिवार्यतः शामिल करता है।

हार्डवेयर, श्रम, भवनों, समन्वय, शासन और प्रवर्तन पर व्यय सभी उत्पादन और संचालन के माध्यम से अवतरित ऊर्जा को शामिल करते हैं। ऊर्जा उपयोग प्रत्यक्ष या अप्रत्यक्ष हो सकता है, लेकिन यदि बाह्य लागत आवश्यक हो तो इसे समाप्त नहीं किया जा सकता।

यह सिद्धांत स्थापित करता है कि □□□ सुरक्षा व्यय गैर-शून्य है लेकिन स्वयं इसकी परिमाण स्थापित नहीं करता। प्रासंगिक तुलना अस्तित्व की नहीं बल्कि पैमाने की है: क्या विस्थापित □□□ व्यय समतुल्य सुरक्षा स्तरों के लिए □□□ व्यय के समीप पहुंचता है? यह इस बात पर निर्भर करता है कि कौन से चैनल विस्थापित व्यय को अवशोषित करते हैं और प्रत्यक्ष हैशिंग के सापेक्ष उनकी ऊर्जा तीव्रता क्या है। मेढ़ ?? यह दावा विकसित करती है कि प्रासंगिक चैनल—□□□ अवसंरचना, सत्यापनकर्ता अतिरेक, शासन समन्वय—समतुल्य सुरक्षा स्तरों के लिए प्रत्यक्ष खनन व्यय के तुलनीय पैमाने पर ऊर्जावान रूप से अवतरित हैं।

5 प्रूफ-ऑफ-वर्क और सुपाठ्य सुरक्षा व्यय

प्रूफ-ऑफ-वर्क प्रणालियों में, सुरक्षा व्यय को ऊर्जा खपत के माध्यम से प्रत्यक्ष रूप से व्यक्त किया जाता है।

माना:

- $\mathcal{H}_t$: प्रति ब्लॉक आवश्यक अपेक्षित हैश (कठिनाई का एक फ़ंक्शन),
- e_t: प्रति हैश जूल,
- c_t: विद्युत मूल्य (□□□/जूल)।

प्रति ब्लॉक अपेक्षित विद्युत लागत है:

$$\mathbb{E}[C_t^{\square\square\square}] = \mathbb{E}[\mathcal{H}_t\, e_t\, c_t] + \mathbb{E}[\square\square\square\square\square\square\square\square_t].$$

k ब्लॉकों पर नियंत्रण की आवश्यकता वाले आक्रमण के लिए, निवारण की आवश्यकता है:

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

पुनर्व्यवस्था एक अंतर्निहित मूल्य सीमा देती है:

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

5.1 प्रोटोकॉल-दृश्य सुरक्षा घनत्व

निर्णायक रूप से, □□□ प्रोटोकॉल $\mathcal{H}_t$ और Π_t को सीधे अवलोकन करते हैं। इसलिए डेमन गणना कर सकता है:

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

निर्गमन की प्रति इकाई का समर्थन करने वाला अपेक्षित अपरिवर्तनीय कार्य।

यह प्रति सिक्के सुरक्षा व्यय का एक सजीव, प्रतिकूल-प्रकट, प्रोटोकॉल-मूल माप प्रदान करता है। प्रूफ-ऑफ-स्टेक प्रणालियों में कोई समतुल्य राशि मौजूद नहीं है।

एक संकेत के रूप में σ_t के खेल-सैद्धांतिक गुण ध्यान देने योग्य हैं। दो प्रश्न उठते हैं। पहला, क्या σ_t को बड़े खनिकों द्वारा जोड़-तोड़ा जा सकता है? चूंकि $\mathcal{H}_t$ कठिनाई द्वारा निर्धारित होता है (कई ब्लॉकों पर एक पिछड़ा औसत), अल्पकालिक जोड़-तोड़ का सीमित प्रभाव होता है; निरंतर गलत प्रस्तुति के लिए किसी भी $\mu < 1/2$ के लिए जोड़-तोड़ लाभ से अधिक दर पर ब्लॉक पुरस्कार छोड़ना आवश्यक होता है। दूसरा, यदि मौद्रिक नीति σ_t के प्रति प्रतिक्रिया करती है तो संतुलन गतिशीलता क्या होती है? यदि निर्गमन σ_t के प्रति प्रतिक्रिया में समायोजित होता है, तो खनिक इसका अनुमान लगाते हैं और तदनुसार हैशरेट को समायोजित करते हैं—एक रणनीतिक प्रतिक्रिया जिसे अनुकूली मौद्रिक तंत्र को ध्यान में रखना चाहिए। इन गतिशीलताओं का विश्लेषण [?] में किया गया है।

टिप्पणी (पिछड़ा संकेत). क्योंकि कठिनाई की गणना कई ब्लॉकों पर एक रोलिंग औसत के रूप में की जाती है (में 2016 ब्लॉक), σ_t तत्काल के बजाय ऐतिहासिक सुरक्षा व्यय को दर्शाता है। हैशपावर में तेज गिरावट—उदाहरण के लिए, एक प्रमुख खनन क्षेत्र का नियामक बंद—कठिनाई एल्गोरिदम के सुधार से पहले पूर्ण कठिनाई समायोजन विंडो तक σ_t को कृत्रिम रूप से ऊंचा छोड़ देती है। जो प्रणालियाँ σ_t को एक अनुकूली संकेत के रूप में उपयोग करती हैं, उन्हें इस पिछड़ेपन का हिसाब देना होगा, या तो रूढ़िवादी प्रतिक्रिया मापदंडों के माध्यम से या अवलोकित ब्लॉक अंतराल भिन्नता जैसे सहायक वास्तविक-समय संकेतों की निगरानी करके।

6 प्रूफ-ऑफ-स्टेक में विस्थापित व्यय

प्रूफ-ऑफ-स्टेक निरंतर हैशिंग को समाप्त करता है लेकिन $\mathbb{E}[V_t]$ तक संसाधन व्यय करने के प्रोत्साहन को नहीं। इसके बजाय, व्यय कई चैनलों में विस्थापित हो जाता है:

- सत्यापनकर्ता पहचान प्रसार और अवसंरचना दोहराव,
- -संचालित अनुकूलन, विलंबता दौड़ और विशेष हार्डवेयर,
- शासन अधिग्रहण, समन्वय और प्रवर्तन,
- अभिरक्षा, कानूनी और अनुपालन ऊपरी व्यय।

माना $C_t^{\text{}}$ सभी ऐसे चैनलों में कुल बाह्य लागत को दर्शाता है। संतुलन सुरक्षा की आवश्यकता है:

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

ये लागतें ऊर्जावान रूप से अवतरित रहती हैं लेकिन प्रोटोकॉल-सुपाठ्य नहीं हैं और ऑडिट या अनुकूलन करना कठिन है।

टिप्पणी (खतरा मॉडल असमानता). उपरोक्त व्यय तुलना मानती है कि आक्रमण एक ही उद्देश्य की ओर निर्देशित हैं: हाल के इतिहास को फिर से लिखने के लिए सक्रिय सर्वसम्मति भागीदारी के पर्याप्त अंश को नियंत्रित करना। हालांकि, और श्रेणीगत रूप से भिन्न आक्रमण वेक्टर का सामना करते हैं। प्रणालियाँ अतिरिक्त रूप से दीर्घ-श्रेणी आक्रमणों के प्रति संवेदनशील हैं: एक विरोधी जो पुराने सत्यापनकर्ता निजी कुंजियाँ प्राप्त करता है (प्रारंभिक प्रतिभागियों, समझौता किए गए एक्सचेंजों, या जमाओं से जो तब से निकाले जा चुके हैं) पिछले युग से नगण्य लागत पर इतिहास को संभावित रूप से फिर से लिख सकता है, क्योंकि उन कुंजियों में कोई निरंतर आर्थिक जोखिम नहीं है। यह आक्रमण में बाधित रूप से महंगा है—ब्लॉकों को फिर से लिखने के लिए पुनर्लिखित श्रृंखला में प्रत्येक ब्लॉक के लिए ऊर्जा को फिर से व्यय करना आवश्यक है, एक अपरिवर्तनीय भौतिक बाधा। किराया-विसर्जन ढांचा चल भागीदारी के लिए संतुलन व्यय को चित्रित करता है; यह इस गुणात्मक रूप से भिन्न आक्रमण वर्ग की असममित लागत को नहीं पकड़ता। प्रणालियाँ इसे कमजोर व्यक्तिपरकता चौकियों या अंतिमता पर सामाजिक सहमति के माध्यम से संबोधित करती हैं, संस्थागत समन्वय को फिर से शुरू करती हैं जिसकी किराया-विसर्जन मॉडल को आवश्यकता नहीं थी।

7 निर्गमन, थ्रूपुट और गलत-आरोपित बाधाएं

एक सामान्य गलत धारणा यह है कि प्रूफ-ऑफ-वर्क अनिवार्य रूप से लेनदेन थ्रूपुट को सीमित करता है। यह सर्वसम्मति को क्षमता नियोजन के साथ भ्रमित करता है। □□□ लीडर चयन और सुरक्षा लागत निर्धारित करता है; थ्रूपुट ब्लॉक आकार, ब्लॉक आवृत्ति और नेटवर्क डिज़ाइन द्वारा निर्धारित होता है।

□□□□□□□ में अवलोकित थ्रूपुट सीमाएं स्पष्ट पैरामीटर विकल्पों और शासन निर्णयों से उत्पन्न होती हैं, न कि स्वयं प्रूफ-ऑफ-वर्क से।

8 मानव-नियंत्रित निर्गमन और रणनीतिक विफलता

मानवीय विवेक पर निर्भर कोई भी निर्गमन तंत्र दोहराए जाने वाले खेल प्रोत्साहन, असममित जानकारी और रणनीतिक अधिग्रहण को प्रस्तुत करता है। समय के साथ, ऐसी प्रणालियाँ विश्वसनीयता क्षरण और अत्यधिक निर्गमन प्रदर्शित करती हैं।

इसके विपरीत, □□□ एक प्रतिकूल-उत्पन्न, गैर-सामाजिक सुरक्षा व्यय संकेत को उजागर करता है। इस संकेत के प्रति एल्गोरिदमिक रूप से प्रतिक्रिया करने वाले निर्गमन तंत्र विवेकाधीन नियंत्रण और संस्थागत ओरेकल से बचते हैं।

9 निष्कर्ष

हमने दर्शाया है कि अनुमति-रहित सर्वसम्मति में संतुलन सुरक्षा व्यय जोखिम में पड़े अपेक्षित बाह्य मूल्य से आबद्ध है। प्रूफ-ऑफ-वर्क इस व्यय को ऊर्जा खपत के माध्यम से प्रत्यक्ष और सुपाठ्य रूप से व्यक्त करता है और विशिष्ट रूप से प्रति निर्गमन इकाई सुरक्षा व्यय का एक प्रोटोकॉल-दृश्य माप प्रदान करता है। प्रूफ-ऑफ-स्टेक संतुलन में ऊर्जा लागतों को समाप्त नहीं करता; यह उन्हें अपारदर्शी और अक्सर कम कुशल संस्थागत रूपों में विस्थापित करता है।

ये परिणाम उन दावों को कमज़ोर करते हैं कि □□□ अनिवार्य रूप से पर्यावरणीय रूप से श्रेष्ठ है और □□□ को सुपाठ्य, प्रतिकूल-प्रकट सुरक्षा के लिए एक विशिष्ट ऑन्टोलॉजिकल सब्सट्रेट के रूप में स्थापित करते हैं। मौद्रिक डिज़ाइन और अनुकूली निर्गमन के लिए निहितार्थ [?] में विकसित किए गए हैं, जो कार्य प्रॉक्सी σ_t को एक अनुकूली निर्गमन संकेत के रूप में उपयोग करने वाले एक ओरेकल-मुक्त दो-लूप तंत्र को निर्दिष्ट करता है। एक एंटी-स्पैम फेडरेटेड मैसेजिंग परत के रूप में बर्न-टू-स्पीक का प्रोटोकॉल-स्तरीय तात्कालिकरण [?] में निर्दिष्ट है।

हवाले

[1] □. □□□□□□□. □□□□□□□□□□ □□□□ □□□□□□□□. □□ □. □□□□□□□□□, □. □□□□□□□□□, □□□ □. □□□□□□□□, □□□□□□□□, □□□□□□□ □ □□□□□□□ □□ □□□ □□□□-□□□□□□□□ □□□□□□□□, □□□□□□ 97–112. □□□□□□ □□□ □□□□□□□□□□□ □□□□□□, 1980.

[2] □. □. □□□□□□□□. □□□ □□□□□□□□□□ □□□□□□□□ □□ □□□ □□□□-□□□□□□□□ □□□□□□□□. □□□□□□□□□ □□□□□□□□□ □□□□□□□, 64(3):291–303, 1974.

[3] □. □□□□□□□. □□□ □□□□□□□□□ □□□□□□□ □□ □□□□□□□□ □□□ □□□ □□□□□□□□□□□. □□□□□□□□ □□ □□□□□□□□□□ □□□□□□□□, 130(3):636–678, 2022.

[4] □. □□□□□□□□□. □□□□□□□□: □ □□□□-□□-□□□□ □□□□□□□□□□□ □□□□ □□□□□□□. 2008. https://bitcoin.org/bitcoin.pdf

[5] □. □□□□□□□□□□□. □□□□□□□□□ □□□□ □□□□□□□□□ □□□□□□□ □□□□□□□□ □□□□□□□□: □ □□□□□□□□□□□□□□ □□□□□□□□□□ □□□□ □□□□□□□-□□□□□□□□□□ □□□□ □□□□□-□□□□□□□□ □□□□□ □□□□□□□□□ □□□□ □□□□□. प्रीप्रिंट, 2026.

[6] □. □□□□□□□□□□□. □□□□□□□□: □ □□□□□□□□□□□□□□□□□-□□□□□□□□□□□ □□□□□□□□□ □□□□ □□□□□□□□□□ □□□□□-□□□□□ □□□□□□□□□□ □□□□ □□□□□□□□□-□□□□□□□□□□ □□□□□□□□. प्रीप्रिंट, 2026.