https://blockstack.org/pox.pdf

स्थानांतरण का प्रमाण श्वेतपत्र v1.0

PoX: बिटकॉइन के साथ ट्रांसफर माइनिंग का सबूत

मुनीब अली

हारून ब्लैंकस्टीन

माइकल जे। फ्रीडमैन *

लुडोविक गैलाब्रु

दिवाकर गुप्ता

जूड नेल्सन

जेसी सोस्लो

पैट्रिक स्टेनली

ब्लॉकस्टैक PBC

https://blockstack.org

11 मई, 2020

सार

सार्वजनिक ब्लॉकचेन के लिए आम सहमति एल्गोरिदम को ब्लॉकचैन स्थिति को सुरक्षित रखने के लिए कंप्यूटिंग या वित्तीय संसाधनों की आवश्यकता होती है। इन एल्गोरिदम द्वारा उपयोग किए जाने वाले खनन तंत्र को मोटे तौर पर विभाजित किया गया है

1. **प्रूफ-ऑफ-वर्क** - जिसमें नोड्स कंप्यूटिंग संसाधनों को समर्पित करते हैं, और
2. **प्रूफ-ऑफ-स्टेक**, जिसमें नोड्स आम सहमति एल्गोरिथ्म में भाग लेने के लिए वित्तीय संसाधन समर्पित करते हैं।

प्रूफ-ऑफ-वर्क और प्रूफ-ऑफ-स्टेक दोनों का इस्तेमाल करने के पीछे उच्चस्तरीय विचार यह है कि किसी भी एक विद्वेषपूर्ण व्यक्ति द्वारा पूरे नेटवर्क पर हमला करने के लिए पर्याप्त कंप्यूटिंग शक्ति या स्वामित्व हिस्सेदारी होना वास्तविकता में असंभव है। प्रूफ़-ऑफ़-वर्क का एक वेरिएंट प्रूफ़-ऑफ़-बर्न है जहाँ खनिक, कंप्यूटिंग संसाधनों के लिए एक प्रॉक्सी के रूप में, प्रूफ़-ऑफ़-वर्क क्रिप्टोकरेंसी "बर्निंग" (नष्ट करना) द्वारा प्रतिस्पर्धा करते हैं।

इस पत्र में, हम एक नया खनन तंत्र पेश करते हैं, जिसे प्रूफ-ऑफ-ट्रांसफर (PoX) कहा जाता है जो प्रूफ-ऑफ-बर्न की सिद्धांत का पालन करता है। PoX एक स्थापित ब्लॉकचैन के प्रूफ-ऑफ-वर्क क्रिप्टोकरेंसी का उपयोग नए ब्लॉकचैन को सुरक्षित करने के लिए करता है। हालांकि, प्रूफ-ऑफ-बर्न की तरह क्रिप्टोकरेंसी को जलाने के बजाय, खनिक, प्रतिबद्ध क्रिप्टोकरेंसी को नेटवर्क में उपलब्ध किसी अन्य प्रतिभागी को स्थानांतरित करते हैं। यह उन नेटवर्क प्रतिभागियों को अनुमति देता है जो नए क्रिप्टोकरेंसी नेटवर्क में मूल्य जोड़ रहे हैं ताकि आम सहमति एल्गोरिथ्म में सक्रिय रूप से भाग लेकर आधार क्रिप्टोकरेंसी में इनाम अर्जित कर सकें।

PoX एक मॉडल को प्रोत्साहित करता है जहां एक बेहद सुरक्षित प्रूफ-ऑफ-वर्क ब्लॉकचैन है, जैसे बिटकॉइन। अन्य नए ब्लॉकचेन को नए प्रूफ-ऑफ-वर्क ब्लॉकचैन के बजाय सुरक्षित प्रूफ-ऑफ-वर्क ब्लॉकचैन के सहारे बढ़ाया जा सकता है। PoX के पास दिलचस्प संपत्ति है, जहां प्रतिभागी नए ब्लॉकचेन नेटवर्क में भाग लेते हुए एक अलग, संभावित रूप से अधिक स्थिर - आधार क्रिप्टोकरेंसी में भुगतान कमा

सकते हैं। यह शुरुआती प्रतिभागियों के लिए प्रोत्साहन प्रदान करके नए ब्लॉकचेन के लिए बूटस्ट्रैपिंग समस्या को हल करने में मदद कर सकता है। इसके अलावा, PoX के पास इकोसिस्टम डेवलपर फंड्स के लिए संभावित उपयोग का मामला है। हम स्टैक्स 2.0 ब्लॉकचेन में PoX का उपयोग करने के लिए एक प्रस्ताव पेश करते हैं।

* प्रिंसटन यूनिवर्सिटी में कंप्यूटर साइंस के प्रोफेसर और ब्लॉकस्टैक पीबीसी के तकनीकी सलाहकार।

1 परिचय

ब्लॉकस्टैक सॉफ़्टवेयर विकसित करने का एक ओपन-सोर्स प्रयास है जो पारंपरिक (केंद्रीकृत) वेब ऍप्लिकेशन्स का विकल्प प्रदान करता है। हम मानते हैं कि वेब के लिए अगला अध्याय एक सार्वजनिक स्वामित्व वाले इंटरनेट का उद्भव है, जिसे सार्वजनिक ब्लॉकचेन के ऊपर बनाया गया है।

सार्वजनिक ब्लॉकचेन के लिए आम सहमति एल्गोरिदम को ब्लॉकचैन स्थिति को सुरक्षित रखने के लिए कंप्यूटिंग या वित्तीय संसाधनों की आवश्यकता होती है। इन एल्गोरिदम द्वारा उपयोग किए जाने वाले खनन तंत्र को मोटे तौर पर विभाजित किया गया है

1. **प्रूफ-ऑफ-वर्क** - जिसमें नोड्स कंप्यूटिंग संसाधनों को समर्पित करते हैं, और
2. **प्रूफ-ऑफ-स्टेक**, जिसमें नोड्स आम सहमति एल्गोरिथ्म में भाग लेने के लिए वित्तीय संसाधन समर्पित करते हैं।

प्रूफ-ऑफ-वर्क और प्रूफ-ऑफ-स्टेक दोनों का इस्तेमाल करने के पीछे उच्चस्तरीय विचार यह है कि किसी भी एक विद्वेषपूर्ण व्यक्ति द्वारा पूरे नेटवर्क पर हमला करने के लिए पर्याप्त कंप्यूटिंग शक्ति या स्वामित्व हिस्सेदारी होना वास्तविकता में असंभव है।

प्रूफ-ऑफ-वर्क के साथ, एक खनिक कुछ "काम" करता है जो बिजली की खपत करता है और डिजिटल मुद्रा में इनाम अर्जित करता है। खनिक, सैद्धांतिक रूप से, बिजली और कंप्यूटिंग शक्ति को नवनिर्मित डिजिटल मुद्रा में परिवर्तित करता है। बिटकॉइन इसका एक उदाहरण है और अब तक का सबसे बड़ा और सबसे सुरक्षित PoW ब्लॉकचेन है।

प्रूफ-ऑफ-स्टेक के साथ, खनिक सहमति एल्गोरिदम में भाग लेने के लिए नई डिजिटल मुद्रा की अपनी होल्डिंग्स का संचय करता हैं और खनिक के खराब व्यवहार को उसके फंड्स को "स्लैश" करके दंडित किया जा सकता है। PoS का उपभोग करने के लिए कम ऊर्जा / बिजली की आवश्यकता होती है और क्रिप्टोकरेंसी धारकों को, जो अपनी होल्डिंग पर इनाम आधार क्रिप्टोकरेंसी में दे सकते हैं । PoW की तुलना में PoS कम सुरक्षित हो सकता है क्योंकि

a. नए नोड्स के लिए विश्वसनीय चैनल की समस्या [1]
b. न्यूनतम लागत के साथ ब्लॉकचैन के कई "नकली" इतिहास बनाने के लिए एक हमलावर की क्षमता [2]

बिटकॉइन अब तक का सबसे सुरक्षित ब्लॉकचेन है। ब्लॉकस्टैक ने अपने शुरुआती दिनों से, खुले और अनुमति रहित नेटवर्क में विश्वास स्थापित करने के लिए एक तंत्र के रूप में बिटकॉइन पर भरोसा किया: 2018 में लॉन्च किए गए स्टैक्स 1.0 ब्लॉकचेन, बिटकॉइन के शीर्ष पर "वर्चुअल ब्लॉकचेन" के रूप में काम करता है।[3] हम मानते हैं कि बिटकॉइन "प्रौद्योगिकी का ध्वज" बन सकता है[4], और अधिकांश लोगों को बिटकॉइन के माध्यम से ही क्रिप्टोकरेंसी को परिचित कराया जाएगा। बिटकॉइन के आसपास डेवलपर इकोसिस्टम का विकास जारी है।

हालांकि, बिटकॉइन ब्लॉकचेन में नई सुविधाओं को जोड़ने से एक चुनौती बन गई है: बिटकॉइन सुरक्षित है क्योंकि यह स्थिर है और यह बदलता नहीं है। हालांकि इसके पास स्क्रिप्टिंग भाषा है, लेकिन यह भाषा बेहद सीमित है। यह डिजाइन द्वारा है - जटिलता जोड़ने से हमले की सतह बढ़ जाती है, जो एक मूलभूत परत के रूप में बिटकॉइन के मूल्य को कम करती है। इसके बावजूद, उपयोगकर्ता के स्वामित्व वाले इंटरनेट के लिए अधिक जटिल सुविधा सेट की आवश्यकता होती है। वेब के इस अगले अध्याय को बनाने वाली ब्लॉकचेन को निम्न कार्य के समर्थन के लिए डिज़ाइन किया जाना चाहिए-

- नए प्रकार के डिजिटल सामान का निर्माण
- नए प्रकार के विकेंद्रीकृत ऍप्लिकेशन्स का प्रबंधन, और
- डेवलपर्स द्वारा अकल्पनीय ऍप्लिकेशन्स डेवलपर्स बनाने के लिए पर्याप्त लचीला होना चाहिए

स्टैक्स ब्लॉकचैन इस ब्लॉकचेन को बनाने का एक प्रयास है, और इसके जीवनकाल में, एक विश्वसनीय नींव के रूप में बिटकॉइन के शीर्ष पर इसका उपयोग करते हुए हमने नए, सुविधा संपन्न ब्लॉकचैन की स्थापना के लिए डिजाइन स्पेस की अनुसंधान की है।

स्टैक्स 1.0 ब्लॉकचेन बिटकॉइन के शीर्ष पर "वर्चुअल ब्लॉकचेन" के रूप में कार्य करता है। स्टैक्स 1.0 में होने वाली प्रत्येक लेनदेन, बिटकॉइन की भी लेनदेन है। स्टैक्स लेनदेन का सभी डेटा बिटकॉइन के मेटाडेटा के भीतर एन्कोड होता है। यह डिजाइन सीमित है;स्टैक्स लेनदेन को बिटकॉइन लेनदेन के साथ बैंडविड्थ साझा करना होगा। स्टैक्स लेनदेन को गैर-खनन ब्लॉकचेन नोड्स, जिनको सत्यापन के लिए खनन पुरस्कार नहीं मिलता, द्वारा अलग से सत्यापित किया जाना चाहिए।

स्टैक 2.0 श्रृंखला[5] की डिजाइन के लिए, SIP-001 में हमने प्रूफ-ऑफ-बर्न (PoB) तंत्र का प्रस्ताव रखा। प्रूफ ऑफ बर्न के साथ, स्टैक्स माइनर्स बिजली की खपत के बजाय क्रिप्टोकरेंसी को नष्ट करके

प्रतिस्पर्धा करते हैं। प्रूफ-ऑफ-बर्न खनिकों को विशेष प्रयोजन के हार्डवेयर के बिना भाग लेने की अनुमति देता है और एक सामान्य प्रूफ-ऑफ-वर्क ब्लॉकचैन की तुलना में नेटवर्क प्रतिभागियों के लिए अधिक पारदर्शिता प्रदान करता है। हालांकि, प्रूफ-ऑफ-वर्क ब्लॉकचैन की तरह, प्रूफ-ऑफ-बर्न विनाशकारी है, ब्लॉकचेन को सुरक्षित करने के लिए खनिकों को मूल्य को नष्ट करने की आवश्यकता होती है।

हालाँकि, PoB एक संभावित बूटस्ट्रैपिंग समस्या से ग्रस्त है। PoB श्रृंखला में खनिकों और नेटवर्क प्रतिभागियों को एक नई क्रिप्टोकरेंसी में पुरस्कृत किया जाता है। हालांकि, PoB श्रृंखला के शुरुआती दिनों में, इस क्रिप्टोकरेंसी में आधार क्रिप्टोकरेंसी, बिटकॉइन जितना मूल्य या सुरक्षा नहीं हो सकती है। PoB श्रृंखला परिपक्व होने से पहले, और नए क्रिप्टोकरेंसी की मूल्य और स्थिरता बढ़ने से पहले, खनिक भाग लेने के लिए बिटकॉइन को नष्ट करने के लिए तैयार नहीं हो सकते हैं।

प्रूफ ऑफ ट्रांसफर। इस पत्र में, हम एक नए खनन तंत्र का परिचय देते हैं, जिसे कहा जाता है प्रूफ-ऑफ-ट्रांसफर (PoX) जो प्रूफ-ऑफ-बर्न (PoB) की अवधारणा को सामान्य करता है। PoX एक नए ब्लॉकचेन को सुरक्षित करने के लिए एक स्थापित ब्लॉकचेन के प्रूफ-ऑफ-वर्क क्रिप्टोकरेंसी का उपयोग करता है। हालांकि, PoB के विपरीत, क्रिप्टोकरेंसी को जलाने के बजाय, खनिक नेटवर्क में किसी अन्य भागीदार के लिए प्रतिबद्ध क्रिप्टोकरेंसी को स्थानांतरित करते हैं। यह नेटवर्क प्रतिभागियों को, जो नए क्रिप्टोक्यूरेंसी नेटवर्क में मूल्य जोड़ रहे हैं, आम सहमति एल्गोरिथ्म में सक्रिय रूप से भाग लेकर आधार क्रिप्टोक्यूरेंसी में पुरस्कार अर्जित करने की अनुमति देता है।

PoX नए ब्लॉकचेन के लिए बूटस्ट्रैपिंग समस्या को हल करने में मदद कर सकता है: प्रतिभागी एक अलग, संभावित रूप से अधिक स्थिर, आधार क्रिप्टोकरेंसी में पुरस्कार प्राप्त कर सकते हैं। नए क्रिप्टोकरेंसी में पुरस्कारों की तुलना में ये पुरस्कार प्रारंभिक भागीदारी के लिए बेहतर प्रोत्साहन हो सकते हैं। नए क्रिप्टोकरेंसी के लिए इस प्रारंभिक मूल्य को स्थापित करने से खनिक की रूचि बढ़ाने में मदद मिल सकती है, जो बदले में नए क्रिप्टोकरेंसी पारिस्थितिकी तंत्र(ecosystem) को विकसित करने में मदद करेगा। नए क्रिप्टोकरेंसी प्रतिभागियों के लिए एक आधार क्रिप्टोकरेंसी में प्रोत्साहन प्रदान करके, PoX निर्भर मूल्य के चक्कर से बच जाता है जो एक नए ब्लॉकचेन के लिए खतरा हो सकता है।

PoX का उपयोग न केवल एक नए क्रिप्टोकरेंसी के धारकों से भागीदारी को प्रोत्साहित करने के लिए किया जा सकता है, लेकिन इसका उपयोग डेवलपर फंड स्थापित करने के लिए भी किया जा सकता है। ये डेवलपर फंड एक नए ब्लॉकचैन के पुरे जीवनकाल में काम लिया जा सकता है। क्योंकि फंड बिटकॉइन की तरह एक अलग क्रिप्टोक्यूरेंसी में होंगे, उस फंड का उपयोग नई क्रिप्टोक्यूरेंसी के मूल्य को प्रभावित किए बिना किया जा सकता है।

2 प्रूफ-ऑफ-ट्रांसफर डिज़ाइन

PoX ब्लॉकचेन को डिजाइन करने के लिए PoX माइनिंग का इस्तेमाल आम सहमति के नियमों के सेट के साथ किया जा सकता है। सर्वसम्मत नियम यह निर्धारित करते हैं कि खनिक एक PoX ब्लॉकचेन के साथ कैसे बातचीत करते हैं और सिस्टम आगे की प्रगति करता है, यानी, ब्लॉकचेन को नए ब्लॉक लिखे जाते हैं। इस पत्र के प्रयोजनों के लिए, PoX माइनिंग बिटकॉइन ब्लॉकचैन को आधार क्रिप्टोकरेंसी के रूप में उपयोग करता है। हालांकि किसी भी प्रूफ-ऑफ-वर्क क्रिप्टोकरेंसी का उपयोग किया जा सकता है, हम बिटकॉइन का उपयोग करने का प्रस्ताव देते हैं क्योंकि यह अब तक सबसे सुरक्षित PoW ब्लॉकचैन है और इसके सुरक्षा गुण वर्तमान में अन्य PoW ब्लॉकचेन से बेहतर हैं।

नाम	**संक्षिप्त शब्द**	**नई क्रिप्टोकरेंसी के लिए खनिक द्वारा की जाने वाली कार्रवाई**
प्रूफ ऑफ वर्क	PoW	संगणना के प्रति बिजली का उपभोग करके।
प्रूफ ऑफ स्टेक	PoS	आधार क्रिप्टोकरेंसी में आर्थिक हिस्सेदारी समर्पित करके।
प्रूफ ऑफ बर्न	PoB	आधार क्रिप्टोकरेंसी को नष्ट करके।
प्रूफ़ ऑफ़ ट्रांसफ़र	PoX	आधार क्रिप्टोकरेंसी स्थानांतरित करके।

तालिका 1: अन्य तंत्रों के साथ प्रूफ ऑफ वर्क की तुलना।

PoX एक खनन तंत्र है जिसे पूरी तरह कार्यात्मक आम सहमति एल्गोरिथ्म के लिए आम सहमति नियमों के एक समूह के साथ जोड़ा जाना चाहिए। PoX खनन स्टैक्स ब्लॉकचैन के लिए सर्वसम्मति एल्गोरिदम के लिए प्रस्तावित प्रूफ-ऑफ-बर्न (PoB) का एक सामान्यीकरण है [6, 5]। एक समरूप आम सहमति नियम का उपयोग PoX के साथ भी किया जा सकता है।।

PoB के साथ, PoX में, सर्वसम्मति नियम एक वेरिफिएबल रैंडम फ़ंक्शन (VRF) का उपयोग करते हुए एक राउंड के विजेता खनिक (यानी, मुखिया) का चयन करते हैं। मुखिया स्टैक्स ब्लॉकचैन के अगले खंड को लिखते हैं और पुरस्कार (नए खनन किए गए स्टैक्स) का टकराव करते हैं। हालांकि, PoX में, पते जलाने के लिए बिटकॉइन भेजने के बजाय, खनिक बिटकॉइन को अन्य नेटवर्क प्रतिभागियों के लिए विशिष्ट पते के एक सेट पर भेजते हैं।

PoX का इस्तेमाल विभिन्न प्रकार के ब्लॉकचेन को डिजाइन करने के लिए, सर्वसम्मति के नियमों और आधार क्रिप्टोकरेंसी कैसे वितरित की जाती है, पर निर्भर करता हैं। नीचे हम दो उपयोग के मामलों पर चर्चा करते हैं:

भागीदारी पुरस्कार: PoX का उपयोग नेटवर्क में मूल्य जोड़ने के लिए एक नई क्रिप्टोक्यूरेंसी के धारकों को पुरस्कृत करने के लिए किया जा सकता हैं। स्टैकिंग मैकेनिज़्म, जो SIP-007 [7] में प्रस्तावित है, वह एक ऐसी योजना है जो स्टैक्स (STX) धारकों, जो स्टैक्स नेटवर्क में भाग लेते हैं और मूल्य जोड़ते हैं, को पुरस्कृत करती है। STX धारक जो STX की कुछ थ्रेसहोल्ड संख्या को नियंत्रित करते हैं, एक हस्ताक्षरित संदेश जारी करने में सक्षम होंगे जो कुछ समय के लिए अपने STX टोकन को लॉक करता हैं, धनराशि प्राप्त करने के लिए एक बिटकॉइन पता निर्दिष्ट करता है, और एक स्टैक्स चेन संस्करण / विशाख(fork) पर वर्तमान रूप में संकेत (वोट) करता हैं। यह जानकारी नेटवर्क पर (ईमानदार) खनिक के लिए उपयोगी होगी। प्रोटोकॉल में खनिक इनाम चक्रों में खनन कर सकते हैं, और प्रत्येक चक्र के लिए, अपनी बिटकॉइन प्रतिबद्धताओं को STX टोकन धारकों को भेजेगा, जिन्होंने इनाम चक्र शुरू होने से पहले ऐसे हस्ताक्षरित संदेश जारी किए थे। खनिक जो STX धारक भी हैं वे अन्य खनिकों पर एक लाभ प्राप्त कर सकते हैं, जो संभावित रूप से खनिक समेकन को जन्म दे सकता है। खंड 4.1 में हम इस संभावित समेकन के लिए संभावित उपायों पर चर्चा करेंगे।

डेवलपर फंड: PoX का इस्तेमाल ब्लॉकचेन इकोसिस्टम में डेवलपर फंड बनाने के लिए किया जा सकता है। डेवलपर फंड कुछ बिटकॉइन वॉलेट (संभवत: एक बहु हस्ताक्षर वॉलेट) को नियंत्रित करेगा, और एक प्रोटोकॉल स्थिरांक (Constant) के रूप में PoX प्रोटोकॉल के वॉलेट पते की आपूर्ति करेगा। खनिक जले हुए पते के बजाय इस पते पर प्रतिबद्ध बिटकॉइन भेजेंगे। प्रोटोकॉल बिटकॉइन स्क्रिप्ट का उपयोग करके, डेवलपर फंड के बिटकॉइन पर कुछ बाध्यताएं लगा सकता है, जैसे, कुछ संख्या के ब्लॉक के लिए फंड को लॉक करना, आदि। किसी भी घटना में, इस इनाम योजना के लिए आवश्यक है कि नेटवर्क सहमत हो कि डेवलपर फंड सिस्टम में एक विश्वसनीय भागीदार होना चाहिए।

3 स्टैक्स 2.0 के लिए PoX खनन प्रस्ताव

यह खंड स्टैक्स 2.0 ब्लॉकचेन के लिए भागीदारी पुरस्कारों के साथ PoX खनन का उपयोग करने के लिए एक प्रस्ताव प्रस्तुत करता है। अतिरिक्त विवरण के लिए, हम रीडर को SIP-007[7] के लिए संदर्भित करते हैं ।

डेवलपर फंड को पुरस्कृत करने के लिए PoX का उपयोग अधिक सरल है, जबकि भागीदारी पुरस्कार के कार्यान्वयन के लिए अतिरिक्त सत्यापन और खनन तंत्र की आवश्यकता होती है।

PoB माइनिंग के सामान्य संचालन के अलावा (SIP-001 [5] देखें), प्रतिभागियों को पुरस्कार वितरित करने की आवश्यकता का मतलब है कि प्रोटोकॉल को उन पतों का सेट निर्धारित करना होगा, जिनसे खनिकों को वैध रूप से फंड ट्रांसफर करना पड़ सकता है। PoB माइनिंग को इन चरणों को करने की आवश्यकता नहीं है, क्योंकि पता हमेशा एक ही होता है, यानी बर्न एड्रेस। हालांकि, भागीदारी पुरस्कार के साथ, नेटवर्क प्रतिभागियों को प्राप्तकर्ता बिटकॉइन पते को मान्य करने में सक्षम होना चाहिए।

SIP-007 में, स्टैकिंग में प्रगति इनाम चक्रों पर होती है। प्रत्येक इनाम चक्र में, बिटकॉइन पतों के सेट को पुन: प्रसारित किया जाता है, ताकि इनाम पते के सेट में प्रत्येक बिटकॉइन पता के पास एक बिटकॉइन ब्लॉक हो, जिसमें खनिक इनाम पते पर फंड हस्तांतरित करेंगे।

स्टैक्स ब्लॉकचैन में भाग लेने वाले खनिक बिटकॉइन को स्थानांतरित करके ब्लॉक का नेतृत्व करने के लिए प्रतिस्पर्धा करते हैं। विशेष स्टैक्स ब्लॉकों के लिए मुखिया को छँटाई द्वारा चुना जाता है, जो भेजे गए बिटकॉइन की मात्रा से भारित होता है (अधिक विवरण के लिए, SIP-001 [5] देखें)। एक इनाम चक्र शुरू होने से पहले, स्टैक्स नेटवर्क को आम सहमति तक पहुंचना चाहिए, जिस पर पते मान्य प्राप्तकर्ता हैं। इस पर सर्वसम्मति तक पहुंचना गैर-तुच्छ है: स्टैक्स ब्लॉकचेन में ही बिटकॉइन ब्लॉकचैन से स्वतंत्र कई गुण हैं, और विशाखाएं (forks), लापता ब्लॉक डेटा आदि का अनुभव हो सकता है, जो सभी आम सहमति तक पहुंचना मुश्किल बनाते हैं। एक चरम उदाहरण के रूप में, एक खनिक पर विचार करें, जो एक ब्लॉक के साथ स्टैक्स श्रृंखला की तलाश करता है जिसमें सभी स्टैक्स होल्डिंग्स का एक बड़ा अंश (जैसे, 100%) रखने का दावा किया गया है, और ब्लॉक प्रतिबद्धताओं को जारी करने के लिए आगे बढ़ते हैं जो सभी शुल्क का भुगतान स्वयं को ही करते हैं। नेटवर्क के अन्य नोड्स यह कैसे पता लगा सकते हैं कि यह खनिक की प्रतिबद्धता के हस्तांतरण अवैध है?

प्रत्येक इनाम चक्र से पहले, स्टैक्स नोड्स तैयार चरण में संलग्न होते हैं, जिसमें दो चीज़ें तय की जाती है:

1. **एंकर ब्लॉक** - एंकर ब्लॉक एक स्टैक्स चेन ब्लॉक है। इनाम चक्र की अवधि के लिए, एंकर ब्लॉक के किसी भी वंशज विशाख(fork) को खनन करने के लिए खनन फंड को उचित इनाम के पते पर स्थानांतरित करना होगा।

2. **रिवार्ड सेट** - रिवार्ड सेट बिटकॉइन पते का सेट है जो इनाम चक्र में धन प्राप्त करेगा। यह सेट एंकर ब्लॉक से स्टैक्स चेन स्टेट का उपयोग करके निर्धारित किया जाता है।

इनाम चक्र के दौरान, खनिक बिटकॉइन श्रृंखला पर ब्लॉक प्रतिबद्धताओं को प्रसारित करके अगले स्टैक ब्लॉक के मुखिया बनने के लिए एक दूसरे के साथ प्रतिस्पर्धा करते हैं। ये ब्लॉक कमिटियाँ बिटकॉइन फंड को या तो बर्न एड्रेस या PoX रिवार्ड एड्रेस पर भेजती हैं।

पता की वैद्यता दो अलग-अलग नियमों के अनुसार निर्धारित की जाती है:

1. यदि कोई खनिक किसी भी चेन टिप का निर्माण कर रहा है जो एंकर ब्लॉक का वंशज नहीं है, तो खनिक के सभी प्रतिबद्धता फंड को बर्न एड्रेस (यानी, फंड्स को जला दिया जाता है) पर भेजा जाना चाहिए।

2. यदि एक खनिक एंकर ब्लॉक के वंशज का निर्माण कर रहा है, तो खनिक को रिवार्ड सेट से 5 पतों के लिए प्रतिबद्धता फंड भेजना चाहिए, जिन्हे इस प्रकार चुना गया हो:

   • रिवार्ड सेट से 5 पतों को चुनने के लिए वेरिफ़िएबल रैंडम फंक्शन (सॉर्टिंग द्वारा भी इस्तेमाल किया जाता है) का उपयोग करें। ये 5 पते इस ब्लॉक के लिए इनाम पते हैं।

   • एक बार एक ब्लॉक के लिए पतों को चुने जाने के बाद, इन पतों को रिवार्ड सेट से हटा दिया जाता है, ताकि इनाम चक्र में भविष्य के ब्लॉक इन पतों को न दोहराएं।

ध्यान दें कि पता चयन के लिए उपयोग किए जाने वाले वेरिफ़िएबल रैंडम फंक्शन (VRF) यह सुनिश्चित करता है कि इनाम के पते चुनने वाले प्रत्येक खनिक द्वारा समान पते चुने जाते हैं। यदि कोई खनिक एक बर्न प्रतिबद्धता को प्रस्तुत करता है जो किसी वैध पते पर फंड नहीं भेजता है, तो उन प्रतिबद्धताओं को बाकी नेटवर्क द्वारा नजरअंदाज कर दिया जाता है (क्योंकि कोई भी स्टैक्स नोड परिणाम निकाल सकता है कि स्थानांतरण पते अमान्य हैं)।

सर्वसम्मति एल्गोरिथ्म की जटिलता को कम करने के लिए, स्टैक्स इनाम चक्र की लंबाई तय की जाती है- यदि चक्र में स्लॉट्स की तुलना में कम पते रिवार्ड सेट में भाग लेते हैं, तो शेष ब्लॉकों के लिए, सभी खनिकों को बर्न पते पर फंड भेजना चाहिए।

तैयार चरण पर अधिक विस्तार के लिए, एंकर ब्लॉक को कैसे चुना जाएगा, और स्टैक्स ब्लॉकचैन लापता एंकर ब्लॉक डेटा से कैसे पुनर्प्राप्त कर सकता है, देखें SIP-007 [7]।

3.1 भागीदारी आधारित इनाम सीमा समायोजन

प्रत्येक इनाम चक्र में 5000 बिटकॉइन पते तक खनिक फंड ट्रांसफर हो सकते हैं। यह सुनिश्चित करने के लिए कि यह संख्या प्रतिभागियों के पूल (तरल STX की 100% भागीदारी को देखते हुए) को कवर करने के लिए पर्याप्त है, भागीदारी के लिए सीमा STX की तरल आपूर्ति का 0.02% (1/5000 वां) होना चाहिए। हालांकि, अगर भागीदारी 100% से कम है, तो इनाम पूल छोटे STX धारकों को स्वीकार कर सकता है। प्रोटोकॉल 2 ऑपरेटिंग स्तरों को निर्दिष्ट करता है :

• **25%** - यदि 0.25 से कम STX_LIQUID_SUPPLY STX इनाम चक्र में भाग लेते हैं, तो x STX को नियंत्रित करने वाले प्रतिभागी पर्स में floor (x / (0.00005 · STX_LIQUID_SUPPLY) पते शामिल हो सकते हैं। अर्थात्, तरल आपूर्ति की न्यूनतम भागीदारी सीमा 1 / 20,000 वाँ भाग है।

• **25% - 100%** - यदि 0.25 · STX LIQUID SUPPLY और 1.0 · STX LIQUID SUPPLY के बीच STX एक इनाम चक्र में भाग लेते हैं तो इनाम थ्रेशोल्ड कम किया जाता है ताकि भरे गए स्लॉट की संख्या को अधिकतम किया जा सके। अर्थात्, भागीदारी के लिए न्यूनतम सीमा T, भाग लेने वाले STX का लगभग 1 / 5,000 वां हिस्सा होगा (10,000 STX के वेतन वृद्धि में समायोजित)।'x' STX को नियंत्रित करने वाले प्रतिभागी पुरस्कार में पुरस्कार सेट में floor (x/T) पते शामिल हो सकते हैं।

यदि एक प्रतिभागी संकेत देकर कई इनाम पते प्रस्तुत करने के लिए पर्याप्त STX को लॉक करता है, लेकिन केवल एक इनाम पते को जमा करता है, उस इनाम पते को इनाम सेट में कई बार शामिल किया जाएगा।

3.2 इनाम के पते जमा करना

पुरस्कार प्रतिभागियों को तीन उद्देश्यों के लिए हस्ताक्षरित संदेशों को प्रसारित करना चाहिए:

1. नेटवर्क को इंगित करना कि कितने इनाम चक्र के लिए कितने STX को लॉक किया जाना चाहिए।
2. एक विशेष श्रृंखला टिप के लिए समर्थन का संकेत दें।
3. पुरस्कार प्राप्त करने के लिए बिटकॉइन पते को निर्दिष्ट करना।

ये संदेश या तो स्टैक्स श्रृंखला या बिटकॉइन श्रृंखला पर प्रसारित किए जा सकते हैं। यदि स्टैक्स श्रृंखला पर प्रसारित किया जाता है, तो इनाम अवधि के लिए एंकर ब्लॉक से पहले स्टैक्स श्रृंखला पर इन संदेशों की पुष्टि की जानी चाहिए। यदि बिटकॉइन श्रृंखला पर प्रसारित किया जाता है, तो

उन्हें तैयार चरण के दौरान प्रसारित किया जा सकता है, लेकिन तैयार चरण खत्म होने से पहले शामिल किया जाना चाहिए।

ये हस्ताक्षरित संदेश अधिकांश 12000 बिटकॉइन ब्लॉक (12 इनाम चक्र या 3 महीने) के लिए मान्य हैं। यदि हस्ताक्षरित संदेश 12000 से कम ब्लॉक लॉक अवधि x निर्दिष्ट करता है, तब हस्ताक्षरित संदेश केवल floor (x / 1000) इनाम चक्रों के लिए स्टैकिंग भागीदारी के लिए मान्य है (न्यूनतम भागीदारी लंबाई एक चक्र: 1000 ब्लॉक है)।

3.3 प्रतिभागी सिग्नलिंग प्रतिनिधिमंडल

प्रतिनिधिमंडल की प्रक्रिया एक स्टैक्स वॉलेट एड्रेस (दर्शाए गए पते) को PoX पुरस्कार प्रोटोकॉल में भाग लेने के लिए एक और पता (प्रतिनिधि पता) नामित करने की अनुमति देती है। यह प्रतिनिधि पता, जब तक प्रतिनिधिमंडल मान्य है, प्रतिनिधित्व पते की ओर से भागीदारी संदेश (यानी, संदेश जो स्टैक्स को लॉक करते हैं, बिटकॉइन इनाम का पता और चेन टिप्स के लिए संकेत समर्थन) को प्रसारित करने में सक्षम है। श्रृंखला युक्तियों के लिए प्रतिनिधि पता संकेत समर्थन होने से, यह प्रतिनिधित्व पते के मालिक को नेटवर्क की सुरक्षा में योगदान करने की अनुमति देता है। यह सिग्नलिंग, सामान्य PoX भागीदारी सिग्नलिंग की तरह, खनिकों पर ब्लॉकचेन स्थिरता पर संभावित हमलों का मुकाबला करता है जो छिपे हुए खदानों को खोजना , अंततः अवैध खदानों, और अन्य प्रकार के खनिक दुर्व्यवहार को छिपाने का प्रयास कर सकते हैं।

सहायक प्रतिनिधिमंडल स्टैक ब्लॉकचेन में दो नए लेनदेन प्रकार जोड़ता है:

प्रतिनिधि निधि - यह लेनदेन एक प्रतिनिधित्व-प्रतिनिधि संबंध शुरू करता है। यह निम्नलिखित डेटा वहन करता है:

- प्रतिनिधि का पता
- एंड ब्लॉक: बिटकॉइन ब्लॉक की ऊंचाई जिस पर यह संबंध समाप्त हो जाता है, जब तक कि बाद में एक प्रतिनिधि निधि लेनदेन रिश्ते को अपडेट नहीं कर सकता है। इस अंतिम ब्लॉक के लिए कोई ऊपरी सीमा नहीं है।
- प्रत्यायोजित राशि: इस पते से STX की कुल राशि जो प्रतिनिधिमंडल की ओर से स्टैकिंग संदेश जारी करने में सक्षम होगी।
- इनाम का पता (वैकल्पिक): एक बिटकॉइन पता जिसे प्रतिनिधि के स्टैकिंग संदेशों में धन प्राप्तकर्ता के रूप में निर्दिष्ट किया जाना चाहिए। यदि अनिर्दिष्ट है, तो प्रतिनिधि पता चुन सकता है।

समाप्त करना - यह लेनदेन एक प्रतिनिधित्व-प्रतिनिधि संबंध को समाप्त करता है। यह निम्नलिखित डेटा वहन करता है:

- प्रतिनिधि का पता

ध्यान दें कि किसी दिए गए प्रतिनिधित्व पते और प्रतिनिधि पते के बीच केवल एक ही सक्रिय प्रतिनिधित्व-प्रतिनिधि संबंध है (यानी, जोड़ी (प्रतिनिधित्व पता, प्रतिनिधि पता) एक रिश्ते की विशिष्ट पहचान करता है)। यदि एक प्रतिनिधित्व-प्रतिनिधि संबंध अभी भी सक्रिय है और प्रतिनिधित्व पता संकेत और एक नया "प्रतिनिधि धन" लेनदेन प्रसारित करता है, तो नए लेनदेन की जानकारी पूर्व संबंध को बदल देती है।

दोनों प्रकार के प्रतिनिधि लेनदेन का प्रतिनिधित्व पते द्वारा हस्ताक्षरित होना चाहिए। ये स्टैक ब्लॉकचेन पर लेनदेन हैं, और एक देशी स्मार्ट अनुबंध के माध्यम से लागू किया जाएगा, स्टैक्स 2.0 उत्पत्ति(Genesis) ब्लॉक के दौरान ब्लॉकचेन में लोड करता है।

4 चल रहे और भविष्य के अनुसंधान

हम सक्रिय रूप से PoX खनन और भागीदारी पुरस्कार के कई पहलुओं पर आगे के शोध में लगे हुए हैं। यह खंड दो ऐसे विषयों पर चर्चा करता है।

4.1 खनिक समेकन को संबोधित करना

PoX जब भागीदारी पुरस्कार के लिए उपयोग किया जाता है, जैसा कि वर्णित है, तो खनिक समेकन हो सकता है। क्योंकि खनिक जो धारकों के रूप में भी भाग लेते हैं, वे उन खनिकों पर एक लाभ प्राप्त कर सकते हैं जो धारकों के रूप में भाग नहीं लेते हैं, खनिकों को नई क्रिप्टोकरेंसी खरीदने और अन्य खनिकों को बाहर निकालने के लिए इसका उपयोग करने के लिए दृढ़ता से प्रोत्साहित किया जाएगा। चरम मामले में, इस समेकन से खनन का केंद्रीकरण हो सकता है, जो सार्वजनिक ब्लॉकचैन के विकेंद्रीकरण लक्ष्यों को कम कर देगा। जब हम इस संभावित समेकन को संबोधित करने के लिए अतिरिक्त तंत्र की सक्रिय रूप से जांच कर रहे हैं, हम यहां दो तंत्रों का प्रस्ताव करते हैं-

समयबद्ध PoX - भागीदारी पुरस्कार माइनर समेकन को प्रोत्साहित करते हैं यदि खनिक नए क्रिप्टोक्यूरेंसी प्राप्त करने के लिए स्थायी लाभ प्राप्त करते हैं। हालाँकि, PoX की समयावधि को सीमित करके, यह लाभ समय के साथ कम हो जाता है। इस योजना में, लॉन्च के x साल बाद भागीदारी पुरस्कार के लिए एक "सूर्यास्त ब्लॉक" निर्धारित किया जाएगा। सूर्यास्त ब्लॉक में,

भागीदारी पुरस्कार बंद हो जाएंगे, और सभी खनिक बिटकॉइन जलाकर प्रतिबद्धताओं का प्रदर्शन करेंगे। अथार्त, सूर्यास्त ब्लॉक के बाद, PoX सिस्टम PoB में परिवर्तित हो जाता है। यह संक्रमण समय के साथ रैखिक (Linear) हो सकता है, बिटकॉइन की प्रतिबद्धता का आधा हिस्सा जला दिया जाएगा और अन्य आधा धारकों को स्थानांतरित किया जाएगा, इत्यादि। इस तरह के एक परिवर्तन के लिए सटीक मापदंडों को सिमुलेशन में समायोजित और अध्ययन किया जा सकता है।

यह योजना नए ब्लॉकचेन के लिए बूटस्ट्रैपिंग समस्या को हल करेगी, खनिकों और धारकों को नेटवर्क में भाग लेने के लिए प्रोत्साहन प्रदान करेगी। फिर, ब्लॉकचेन के लिए प्राकृतिक उपयोग के मामले विकसित होने और लाभ प्राप्त करने के लिए, PoX प्रणाली धीरे-धीरे बड़े पैमाने पर हो सकती है।

विश्वसनीय खनिक सेट - भागीदारी पुरस्कारों के कारण मामूली समेकन एक खतरा नहीं है यदि खनिकों को धारकों के रूप में भाग लेने से प्रतिबंधित किया जाता है (अर्थात, खनिक PoX पुरस्कार प्राप्त नहीं कर सकते हैं)। हालांकि, खुले और विकेंद्रीकृत प्रणालियों में, यह निर्धारित करना आसान नहीं है कि किसी दिए गए बटुए का पता किसी अन्य प्रतिभागी का है या नहीं। यह गारंटी प्रदान करने के लिए कि खनिक और धारक अलग-अलग हैं, एक नया ब्लॉकचैन संभावित खनिकों के सेट को एक विश्वसनीय सेट तक सीमित कर सकता है (जिसे कुछ अन्य विश्वसनीय इकाई के माध्यम से बूटस्ट्रैप किया जा सकता है)। इन खनिकों को विश्वसनीय संस्था द्वारा निरीक्षण करना होगा, और अनुपालन सुनिश्चित करने के लिए अन्य प्रणालियों की आवश्यकता होगी (जैसे, कानूनी प्रक्रिया)। हमारे उद्देश्यों के लिए, एक विश्वसनीय माइनर सेट एक खुले सार्वजनिक ब्लॉकचैन के हमारे लक्ष्यों को कम कर देगा, और परिणामस्वरूप ब्लॉकचैन हमारे इच्छित प्रणाली की तुलना में एक संघबद्ध प्रणाली की तरह कार्य करना शुरू कर देगा।।

4.2 बिटकॉइन बैंडविड्थ

क्योंकि PoX खनिकों को सर्वसम्मति एल्गोरिथ्म में भाग लेने के लिए बिटकॉइन लेनदेन भेजना चाहिए और PoX पुरस्कार भेजना चाहिए, PoX खनन कुछ बिटकॉइन लेनदेन बैंडविड्थ पर कब्जा कर लेगा। क्योंकि बिटकॉइन बैंडविड्थ डिजाइन द्वारा सीमित है, सुरक्षा आवश्यकताओं को देखते हुए, नए PoX ब्लॉकचेन को अपने बैंडविड्थ उपयोग आवश्यकताओं को कम करने की आवश्यकता है। SIP-007 प्रतिभागियों की संख्या को सीमित करके, एक STX होल्डिंग सीमा का उपयोग करके ऐसा करता है। बैंडविड्थ सीमाओं को संबोधित करने के अन्य तरीके भी संभव हैं, जैसे, बिटकॉइन और नए ब्लॉकचेन के बीच प्रकाश व्यवस्था(lighting channels)। बिटकॉइन लेनदेन परत पर अनुकूलन भी संभव हो सकता है, जो PoX लेनदेन के लिए आवश्यक कुल आकार को कम

करेगा।हम बिटकॉइन परत पर आकार में कमी और क्रॉस-चेन चैनलों को सक्षम करने के लिए बिजली में संभावित संशोधनों की खोज कर रहे हैं।

संदर्भ

[१] जे। नेल्सन, "PoS ब्लॉकचेन को सर्वसम्मति के लिए विषय की आवश्यकता है," ०३ २०१els।

https://forum.blockstack.org/t/pos-blockchains-require-subjectivity-to-reach-आम सहमति / 762।

[2] ए Poelstra, "स्टेक और आम सहमति पर," 03 2015 https://download.wpsoftware.net/bitcoin/

pos.pdf

[३] ब्लॉकस्टैक PBC, "ब्लॉकस्टैक-कोर: v20.0.8.1," ० 201 २०१ ९।

https://github.com/blockstack/

ब्लॉकस्टैक-कोर / ट्री / v20.0.8.1।

[४] बीएस श्रीनिवासन, "बिटकॉइन प्रौद्योगिकी का ध्वज बन जाता है," १ २०२०।

https://nakamoto.com/

बिटकॉइन-द-फ्लैग-ऑफ-टेक्नोलॉजी /।

[५] जे। नेल्सन और ए। ब्लैंकस्टीन, "एसआईपी ००१: बर्न इलेक्शन,"

https://github.com/blockstack/

ब्लॉकस्टैक-कोर / ब्लॉब / डेवलप / एसआईपी / sip-001-burn-election.md।

[६] एम। अली, जे। नेल्सन, ए। ब्लैंकस्टीन, आर। शीया, और एम.जे. फ्रीडमैन, "ब्लॉकस्टैक टेक्निकल व्हाइटपर v2.0,"

05 2019 । https://blockstack.org/whitepaper.pdf

[[] एम। अली, ए। ब्लैंकस्टीन, एमजे फ्रीडमैन, डी। गुप्ता, जे। नेल्सन, जे। सोस्लो और पी। स्टेनली, "एसआईपी ००7: स्टैक-

आईएनजी सहमति , "https://github.com/blockstack/blockstack-core/blob/develop/sip/

sip-007-stacking-consanim.md।