प्रस्तावना

एसआईपी (SIP) नंबर: 007

शीर्षक: स्टैकिंग सहमति (Stacking Consensus)

लेखक: मुनीब अली muneeb@blockstack.com, आरोन ब्लैंकस्टीन aaron@blockstack.com, माइकल जे फ्रीडमैन mfreed@cs.princeton.edu, दिवाकर गुप्ता diwaker@blockstack.com, जूड नेल्सन jude@blockstack.com, जेसी सोस्लाो jesse@blockstack.com, पैट्रिक स्टेनली patrick@blockstack.com

विचार: तकनीकी

प्रकार: आम सहमति (Consensus)

स्थिति: सत्यापित

बनाया गया: 14 जनवरी 2020

साइन-ऑफ: जूड नेल्सन jude@stacks.org, तकनीकी संचालन समिति के अध्यक्ष

चर्चा: https://github.com/stacksgov/sips

सार

यह SIP एक नया सर्वसम्मति एल्गोरिथ्म प्रस्तावित करता है, जिसे स्टैकिंग कहा जाता है, जो एक नए ब्लॉकचैन को सुरक्षित करने के लिए एक स्थापित ब्लॉकचेन के प्रूफ-ऑफ-वर्क क्रिप्टोकरेंसी का उपयोग करता है। स्टैकिंग सर्वसम्मति एल्गोरिथ्म का एक आर्थिक लाभ यह है कि नए क्रिप्टोक्यूरेंसी के धारक आधार क्रिप्टोक्यूरेंसी (base cryptocurrency) में आम सहमति एल्गोरिथ्म में सक्रिय रूप से भाग लेकर इनाम अर्जित कर सकते हैं।

यह SIP स्टैक्स ब्लॉकचैन के खनन तंत्र (mining mechanism) को बदलने का प्रस्ताव करता है। SIP-001 ने प्रूफ-ऑफ-बर्न (PoB) पेश किया, जहां एक नई क्रिप्टोक्यूरेंसी के खनन में भाग लेने के लिए एक आधार क्रिप्टोक्यूरेंसी को नष्ट कर दिया जाता है। इस प्रस्ताव का तर्क है कि प्रूफ-ऑफ-ट्रांसफर (PoX) नामक एक नया खनन तंत्र प्रूफ-ऑफ-बर्न में सुधार होगा।

प्रूफ-ऑफ-ट्रांसफर के साथ, आधार क्रिप्टोक्यूरेंसी को नष्ट करने के बजाय, खनिक को एल्गोरिथ्म में भाग लेने वाले नए क्रिप्टोक्यूरेंसी के मौजूदा धारकों को आधार क्रिप्टोक्यूरेंसी को वितरित करने की आवश्यकता होती है। इसलिए, नए क्रिप्टोक्यूरेंसी के मौजूदा धारकों को भाग लेने, नेटवर्क के लिए उपयोगी काम करने और पुरस्कार प्राप्त करने के लिए एक आर्थिक प्रोत्साहन है।

प्रूफ-ऑफ-ट्रांसफर आधार क्रिप्टोक्यूरेंसी को जलाने से बचता है जो आधार क्रिप्टोक्यूरेंसी की कुछ आपूर्ति को नष्ट कर देता है। सामान्य रूप से स्टैकिंग को एक अधिक कुशल (“efficient”) एल्गोरिदम के रूप में देखा जा सकता है, जहां एक मूल्यवान संसाधन (जैसे बिजली या आधार क्रिप्टोक्यूरेंसी) को नष्ट करने के बजाय, नए क्रिप्टोक्यूरेंसी के धारकों को मूल्यवान संसाधन वितरित किया जाता है।
यह SIP बिटकॉइन को आधार क्रिप्टोकरेंसी के रूप में उपयोग करके स्टैक्स ब्लॉकचैन के लिए स्टैकिंग सर्वसम्मति एल्गोरिथ्म के एक संभावित कार्यान्वयन का वर्णन करता है।

परिचय

सार्वजनिक ब्लॉकचेन के लिए आम सहमति एल्गोरिदम को ब्लॉकचेन राज्य को सुरक्षित करने के लिए कम्प्यूटेशनल या वित्तीय संसाधनों की आवश्यकता होती है। इन एल्गोरिदम द्वारा उपयोग किए जाने वाले खनन तंत्र को मोटे तौर पर प्रूफ-ऑफ-वर्क (PoW), में विभाजित किया जाता है, जिसमें नोड्स कम्प्यूटेशनल संसाधनों को समर्पित करते हैं, और प्रूफ-ऑफ-स्टेक (PoS), जिसमें नोड्स वित्तीय संसाधनों को समर्पित करते हैं। प्रूफ-टू-वर्क और प्रूफ-ऑफ-स्टेक दोनों के पीछे का उद्देश्य किसी भी दुर्भावनापूर्ण अभिनेता के लिए व्यावहारिक रूप से व्यावहारिक बनाना है, जिसके पास नेटवर्क पर हमला करने के लिए पर्याप्त कम्प्यूटेशनल शक्ति या स्वामित्व हिस्सेदारी है।
प्रूफ-ऑफ-वर्क में एक खनिक (miner) कुछ काम (“work”) करता है जो बिजली की खपत करता है और डिजिटल मुद्रा से पुरस्कृत होता है। माइनर, सैद्धांतिक रूप से, बिजली और कंप्यूटिंग शक्ति को नए खनन डिजिटल मुद्रा में परिवर्तित कर रहा है। बिटकॉइन इसका एक उदाहरण है और अब तक का सबसे बड़ा और सबसे सुरक्षित PoW ब्लॉकचेन है।
प्रूफ-ऑफ-स्टेक के साथ खनिकों (miners) ने सर्वसम्मति एल्गोरिथ्म में भाग लेने के लिए एक नई डिजिटल मुद्रा की अपनी हिस्सेदारी को दांव पर लगाया और खराब व्यवहार को माइनर के फंड को "स्लैश" करके दंडित किया जा सकता है। PoS को उपभोग करने के लिए कम ऊर्जा / बिजली की आवश्यकता होती है और यह नई क्रिप्टोक्यूरेंसी के धारकों को दे सकता है जो नए क्रिप्टोक्यूरेंसी में अपने होल्डिंग्स पर इनाम देने में भाग लेते हैं।
इस SIP में हम स्टैकिंग नामक एक नया सर्वसम्मति एल्गोरिथ्म पेश करते हैं। स्टैकिंग सर्वसम्मति एल्गोरिथ्म एक नए प्रकार के खनन तंत्र का उपयोग करता है जिसे *प्रूफ-ऑफ-ट्रांसफर* (PoX) कहा जाता है। PoX के साथ खनिक बिजली और कंप्यूटिंग शक्ति को नए खनन टोकन में परिवर्तित नहीं कर रहे हैं, और न ही वे अपनी क्रिप्टोकरेंसी को रोक रहे हैं। बल्कि वे एक नए, अलग ब्लॉकचेन को सुरक्षित करने के लिए एक मौजूदा PoW क्रिप्टोक्यूरेंसी का उपयोग करते हैं।
यह SIP वर्तमान में एक मसौदा है और स्टैक्स ब्लॉकचेन के खनन तंत्र को प्रूफ-ऑफ-बर्न (SIP-001) से प्रूफ-ऑफ-ट्रांसफर में बदलने का प्रस्ताव करता है।

PoX खनन तंत्र प्रूफ-ऑफ-बर्न (PoB) खनन का एक संशोधन है (Blockstack Technical Whitepaper और SIP-001 देखें)। प्रूफ-ऑफ-बर्न माइनिंग में खनन में भाग लेने के लिए खनिक एक आधार क्रिप्टोक्यूरेंसी को जलाते हैं - एक नई क्रिप्टोक्यूरेंसी की टकसाल इकाइयों को आधार क्रिप्टोक्यूरेंसी (base cryptocurrency) को प्रभावी ढंग से नष्ट कर देते हैं। **प्रूफ-ऑफ-ट्रांसफर में आधार क्रिप्टोक्यूरेंसी को नष्ट करने के बजाय खनिक (miners) नए क्रिप्टोक्यूरेंसी के मालिकों को इनाम के रूप में आधार क्रिप्टोक्यूरेंसी को स्थानांतरित करते हैं।** स्टैक्स ब्लॉकचैन के मामले में, खनिकों स्टैक्स के मालिकों को बिटकॉइन हस्तांतरित करेंगे ताकि खनिकों को नव-खनन किए गए स्टैक्स टोकन प्राप्त हों। प्रूफ-ऑफ-ट्रांसफर के सुरक्षा गुण प्रूफ-ऑफ-बर्न के बराबर हैं।

विनिर्देश

बिटकॉइन के साथ स्टैकिंग

स्टैकिंग सर्वसम्मति प्रोटोकॉल में, हमें ब्लॉक क्रिप्टोक्यूरेंसी को प्रूफ-ऑफ-वर्क ब्लॉकचेन की आवश्यकता होती है। स्टैकिंग के इस प्रस्तावित कार्यान्वयन में हम मानते हैं कि PoW क्रिप्टोक्यूरेंसी बिटकॉइन है, यह देखते हुए यह अब तक का सबसे सुरक्षित PoW ब्लॉकचैन है। सैद्धांतिक रूप से अन्य PoW ब्लॉकचेन का उपयोग किया जा सकता है, लेकिन बिटकॉइन के सुरक्षा गुण वर्तमान में अन्य PoW ब्लॉकचेन से बेहतर हैं।

PoB के साथ PoX में प्रोटोकॉल एक वेरिफाइयबल रैंडम फ़ंक्शन (सत्यापन-यादृच्छिक-फ़ंक्शन / verifiable random function / VRF) का उपयोग करके एक राउंड के विजेता माइनर (यानी leader) का चयन करता है। नेता (leader) स्टैक्स ब्लॉकचेन का नया ब्लॉक लिखता है और पुरस्कार (नए खनन किए गए स्टैक्स) बनाता है। हालांकि, बिटकॉइन को जलाने के पते (burn address) पर भेजने के बजाय, बिटकॉइन को स्टैक्स (STX) टोकन धारकों के लिए विशिष्ट पते के एक सेट पर भेजा जाता है जो नेटवर्क में मूल्य जोड़ रहे हैं। इस प्रकार, नष्ट होने के बजाय, खनन प्रक्रिया में उपभोग किए जाने वाले बिटकॉइन उत्पादक स्टैक्स धारकों के पास जाते हैं, जो स्टैक्स की उनकी होल्डिंग और स्टैकिंग एल्गोरिदम में भागीदारी के आधार पर एक इनाम के रूप में मिलते हैं।

स्टैकिंग सर्वसम्मति एल्गोरिथ्म (Stacking Consensus Algorithm)

PoB माइनिंग (SIP-001 देखें), के सामान्य कार्यों के अलावा, स्टैकिंग सर्वसम्मति एल्गोरिथ्म को उन पतों के सेट को निर्धारित करना होगा जो खनिकों को वैध रूप से फंड ट्रांसफर कर सकते हैं। PoB माइनिंग को इन चरणों को करने की आवश्यकता नहीं है, क्योंकि पता हमेशा एक ही होता है - बर्न एड्रेस (burn address)। हालांकि, स्टैकिंग के साथ, नेटवर्क प्रतिभागियों को भेजे जाने वाले पते को मान्य करने में सक्षम होना चाहिए।

स्टैकिंग सर्वसम्मति में प्रगति *इनाम चक्रों* पर होती है। प्रत्येक इनाम चक्र में, बिटकॉइन पतों का एक सेट आवर्ती होता है, जैसे कि रिवार्ड पतों के सेट में प्रत्येक बिटकॉइन पते में एक बिटकॉइन ब्लॉक होता है जिसमें खनिक इनाम के पते पर धन हस्तांतरित करेंगे।
एक इनाम चक्र के लिए अर्हता प्राप्त करने के लिए, एक STX धारक (STX holder) को चाहिए:

- अनलॉक किए गए स्टैक्स टोकन के कुल शेयर का >= 0.02% के साथ एक स्टैक्स वॉलेट को नियंत्रित करें (वर्तमान में, ~ 47 करोड़ अनलॉक किया हुआ स्टैक्स टोकन, जिसका अर्थ है कि इसे ~94 हज़ार स्टैक्स की आवश्यकता होगी)। यह सीमा स्तर स्टैकिंग प्रोटोकॉल में सहभागिता स्तरों के आधार पर समायोजित होता है।
- इनाम चक्र शुरू होने से पहले एक हस्ताक्षरित संदेश प्रसारित करें:
    - एक प्रोटोकॉल-निर्दिष्ट लॉकअप अवधि के लिए संबंधित स्टैक्स टोकन को लॉक करता है।
    - निधियों को प्राप्त करने के लिए एक बिटकॉइन पता निर्दिष्ट करता है।
    - एक स्टैक्स श्रृंखला टिप पर वोट।

स्टैक्स ब्लॉकचैन में भाग लेने वाले खनिक बिटकॉइन को स्थानांतरित करके ब्लॉक का नेतृत्व करने के लिए प्रतिस्पर्धा (competition) करते हैं। विशेष रूप से स्टैक्स ब्लॉक के लिए नेताओं (leaders) को भेजे गए बिटकॉइन की मात्रा से भारित करके चुना जाता है (देखें SIP-001)। एक इनाम चक्र (reward cycle) शुरू होने से पहले, स्टैक्स नेटवर्क को आम सहमति (consensus) तक पहुंचना चाहिए, जिस पर पते मान्य प्राप्तकर्ता (valid recipients) हैं। इस पर आम सहमति तक पहुंचना गैर-तुच्छ (non-trivial) है: स्टैक्स ब्लॉकचेन में स्वयं बिटकॉइन ब्लॉकचेन से स्वतंत्र कई गुण हैं, और कांटे (forks), लापता ब्लॉक डेटा (missing block data) आदि का अनुभव हो सकता है, जो सभी आम सहमति तक पहुंचना मुश्किल बनाते हैं। एक चरम उदाहरण के रूप में, एक माइनर पर विचार करें जो सभी ब्लॉक होल्डिंग्स के एक बड़े अंश (जैसे, 100%) को रखने का दावा करने वाले ब्लॉक के साथ स्टैक्स श्रृंखला की विभाजन (forks the Stacks chain) करता है, और ब्लॉक प्रतिबद्धताओं (block commitments) को जारी करने के लिए आय करता है कि सभी फीस का भुगतान खुद करें। नेटवर्क के अन्य नोड्स यह कैसे पता लगा सकते हैं कि यह माइनर की प्रतिबद्धता (miner's commitment) के हस्तांतरण अवैध हैं?
स्टैकिंग एल्गोरिथ्म इसे दो-चरण चक्र के साथ संबोधित करता है। प्रत्येक इनाम चक्र से पहले, स्टैक्स नोड्स एक *तैयार चरण* (prepare phase) में संलग्न होते हैं, जिसमें दो आइटम तय किए जाते हैं:

1. **एंकर ब्लॉक** – एंकर ब्लॉक एक स्टैक्स चेन ब्लॉक है। इनाम चक्र (reward cycle) की अवधि के लिए, एंकर ब्लॉक के किसी भी वंशज कांटे (descendant forks) को खनन (mining) करने के लिए खनन धन (mining funds) को उचित इनाम के पते (appropriate reward addresses) पर स्थानांतरित करना होगा।
2. **इनाम सेट** / **रिवॉर्ड सेट** (reward set) - इनाम सेट बिटकॉइन पते का सेट है जो इनाम चक्र में धन (funds) प्राप्त करेगा। यह सेट एंकर ब्लॉक से स्टैक्स चेन स्टेट का उपयोग करके निर्धारित किया जाता है।

इनाम चक्र (rewards cycle) के दौरान, खनिक (miners) बिटकॉइन श्रृंखला पर *ब्लॉक प्रतिबद्धताओं* (block commitments) को प्रसारित करके अगले स्टैक्स ब्लॉक के नेता (leader) बनने के लिए एक दूसरे के साथ प्रतिस्पर्धा (compete) करते हैं। ये ब्लॉक कमिटमेंट बिटकॉइन फंड्स को या तो बर्न एड्रेस या PoX रिवार्ड एड्रेस भेजते हैं।
पता वैधता (address validity) दो अलग-अलग नियमों के अनुसार निर्धारित की जाती है:

1. यदि कोई माइनर किसी भी चेन टिप का निर्माण कर रहा है, जो एंकर ब्लॉक का वंशज नहीं है, तो माइनर के सभी प्रतिबद्धता फंड (commitment funds) को जला दिया जाना चाहिए।
2. यदि कोई माइनर एंकर ब्लॉक के वंशज का निर्माण कर रहा है, तो माइनर को इनाम के सेट से 2 पतों पर प्रतिबद्धता फंड (commitment funds) भेजना चाहिए, जो की इस प्रकार चुना जाएगा:
    - रिवार्ड सेट से 2 पतों को चुनने के लिए वेरिफाइयबल रैंडम फ़ंक्शन (सॉर्टिंग द्वारा भी इस्तेमाल किया जाता है) का उपयोग करें। ये 2 पते इस ब्लॉक के लिए इनाम के पते हैं।
    - एक बार जब किसी ब्लॉक के लिए पते चुन लिए जाते हैं, तो इन पतों को रिवार्ड सेट से हटा दिया जाता है, ताकि इनाम चक्र में भविष्य के ब्लॉक पतों को न दोहराएं।

ध्यान दें कि पते के चयन के लिए उपयोग किए जाने वाले वेरिफाइयबल रैंडम फ़ंक्शन (VRF) सुनिश्चित करता है कि इनाम के पते का चयन करने वाले प्रत्येक खनिक द्वारा समान पते चुने जाते हैं। यदि कोई माइनर बर्न कमिटमेंट को सबमिट करता है जो फंड को वैध पते पर *नहीं भेजता है*, तो उन प्रतिबद्धताओं को बाकी नेटवर्क द्वारा नजरअंदाज कर दिया जाता है (क्योंकि अन्य नेटवर्क प्रतिभागी यह कह सकते हैं कि ट्रांसफर एड्रेस अमान्य हैं)।
सर्वसम्मति एल्गोरिथ्म (consensus algorithm) की जटिलता को कम करने के लिए, स्टैकिंग रिवॉर्ड साइकल की लंबाई तय है --- यदि साइकल में स्लॉट्स जितने है उसमें से कम पतों में स्टैकिंग रिवार्ड्स में भाग लेते हैं, तो बचे हुए स्लॉट *बर्न एड्रेस* (burn address) से भरे हुए हैं। *बर्न एड्रेस* निश्चित अंतराल (fixed intervals) पर माइनर कमिटमेंट में शामिल हैं (उदाहरण के लिए, यदि इनाम चक्र के लिए 1000 बर्न एड्रेस हैं, तो प्रत्येक माइनर कमिटमेंट में आउटपुट के रूप में 1 बर्न एड्रेस होगा)।

भागीदारी के आधार पर रिवार्ड थ्रेशोल्ड को समायोजित (Adjust) करना

प्रत्येक इनाम चक्र 4000 बिटकॉइन पते (2000 बर्न ब्लॉक चक्र में 2 पते) तक खान राशि (miner funds) को स्थानांतरित कर सकता है। यह सुनिश्चित करने के लिए कि यह संख्या प्रतिभागियों के पूल (liquid STX की 100% भागीदारी को देखते हुए) को कवर करने के लिए पर्याप्त है, भागीदारी का हिस्सा liquid STX आपूर्ति (supply) का 0.025% (1/4000 वां) होना चाहिए। हालांकि, अगर भागीदारी 100% से *कम* है, तो इनाम पूल कम STX धारकों को स्वीकार कर सकता है। स्टैकिंग प्रोटोकॉल 2 **ऑपरेटिंग स्तर** निर्दिष्ट करता है:

- **25%** यदि `0.25 * STX_LIQUID_SUPPLY` से कम STX एक इनाम चक्र में भाग लेते हैं, तो x STX को नियंत्रित करने वाले प्रतिभागी वॉलेट में इनाम सेट में `floor(x / (0.0000625*STX_LIQUID_SUPPLY))` पते शामिल हो सकते हैं। जिसका अर्थ है, न्यूनतम भागीदारी सीमा है तरल आपूर्ति (liquid supply) का 1 / 16,000 वां भाग।
- **25% -100%** यदि `0.25 * STX_LIQUID_SUPPLY` और `1.0 * STX_LIQUID_SUPPLY` के बीच में STX इनाम चक्र में भाग लेते हैं, तो भरे गए स्लॉट की संख्या को अधिकतम करने के लिए इनाम सीमा को अनुकूलित (optimize) किया जाता है। जिसका अर्थ है, भागीदारी के लिए न्यूनतम सीमा T लगभग 1 / 4,000 वां प्रतिभागी STX (10,000 STX की वृद्धि में समायोजित) होगी। x STX को नियंत्रित करने वाले प्रतिभागी वॉलेट में पुरस्कार सेट (reward set) में `floor(x / T)` पते शामिल हो सकते हैं।

अगर एक स्टेकर (Stacker) कई इनाम पते प्रस्तुत करने के लिए संकेत करते हुए 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।

इनाम का पता जमा करना और चैन टिप सिग्नल करना

स्टैकिंग प्रतिभागियों को तीन उद्देश्यों के लिए हस्ताक्षरित संदेशों (signed messages) को प्रसारित करना चाहिए:

1. नेटवर्क को इंगित करने के लिए कि कितने STX को लॉक किया जाना चाहिए, और कितने रिवार्ड साइकल के लिए।
2. एक विशेष श्रृंखला टिप (chain tip) के लिए समर्थन का संकेत देने के लिए।
3. स्टैकिंग पुरस्कार प्राप्त करने के लिए बिटकॉइन पते को निर्दिष्ट करने के लिए।

ये संदेश या तो स्टैक्स श्रृंखला (Stacks chain) या बिटकॉइन श्रृंखला (Bitcoin chain) पर प्रसारित किए जा सकते हैं। यदि स्टैक्स श्रृंखला पर प्रसारित किया जाता है तो इनाम अवधि (reward period) के लिए एंकर ब्लॉक से *पहले* स्टैक्स श्रृंखला पर इन संदेशों की पुष्टि (confirm) की जानी चाहिए। यदि बिटकॉइन श्रृंखला पर प्रसारित किया जाता है तो उन्हें तैयार चरण (prepare phase) के दौरान प्रसारित किया जा सकता है, लेकिन तैयार चरण खत्म होने से पहले शामिल किया जाना चाहिए।
ये हस्ताक्षरित संदेश (signed messages) अधिकांश 12 इनाम चक्रों (25200 बिटकॉइन ब्लॉक या ~7 महीने) के लिए मान्य हैं। यदि हस्ताक्षरित संदेश 25200 ब्लॉक से कम लॉकअप अवधि x निर्दिष्ट करता है, तो हस्ताक्षरित संदेश केवल `floor(x / 2100)` इनाम चक्र के स्टैकिंग भागीदारी (Stacking participation) के लिए मान्य है (न्यूनतम भागीदारी लंबाई है एक चक्र: 2100 ब्लॉक)।

एंकर ब्लॉक और पुरस्कार सहमति (Anchor Blocks and Reward Consensus)

स्टैकिंग एल्गोरिदम के **तैयार चरण** में, खनिक और नेटवर्क प्रतिभागी एंकर ब्लॉक और रिवार्ड सेट का निर्धारण करते हैं। तैयारी चरण इनाम चक्र शुरू होने से *पहले* बिटकॉइन ब्लॉकों की एक विंडो `w` है (जैसे, यह विंडो 100 बिटकॉइन ब्लॉक हो सकती है)।

उच्च-स्तर पर, नोड्स यह निर्धारित करते हैं कि चरण के दौरान `F*w` ब्लॉक द्वारा किसी भी ब्लॉक की पुष्टि (confirmation) की गई थी या नहीं, जहां `F` एक बड़ा अंश है (जैसे, `0.8`)। एक बार जब विंडो `w` समय `cur` पर बंद हो जाती है, तो स्टैक्स नोड्स संभावित एंकर ब्लॉक को कैसे पाते हैं यह निम्न सूडोकोड में वर्णित हैं:

```
def find_anchor_block(cur):
  blocks_worked_on = get_all_stacks_blocks_between(cur - w, cur)

  # get the highest/latest ancestor before the PREPARE phase for each block worked
  # on during the PREPARE phase.

  candidate_anchors = {}
  for block in blocks_worked_on:
    pre_window_ancestor = last_ancestor_of_block_before(block, cur - w)
    if pre_window_ancestor is None:
      continue
    if pre_window_ancestor in candidate_anchors:
      candidate_anchors[pre_window_ancestor] += 1
    else:
      candidate_anchors[pre_window_ancestor] = 1

  # if any block is confirmed by at least F*w, then it is the anchor block.
  for candidate, confirmed_by_count in candidate_anchors.items():
    if confirmed_by_count >= F*w
      return candidate

  return None
```

ध्यान दें कि सबसे अधिक एक ही एंकर ब्लॉक हो सकता है (जब तक `F > 0.5` है), क्योंकि:

- तैयार चरण (prepare phase) में प्रत्येक `w` ब्लॉक में अधिकांश एक उम्मीदवार पूर्वज (candidate ancestor) हैं।
- एंकर ब्लॉक के लिए पुष्टियों (confirmations) की कुल संभावित संख्या `w` है।
- यदि किसी ब्लॉक की पुष्टि `>= 0.5*w` से होती है, तो किसी अन्य ब्लॉक की पुष्टि `< 0.5*w` द्वारा की जानी चाहिए।

तैयार चरण (prepare phase) और `F` के लिए उच्च सीमा, स्टैकिंग सर्वसम्मति प्रोटोकॉल (Stacking consensus protocol) को प्राकृतिक कांटे (natural forks), लापता ब्लॉक डेटा और संभावित रूप से दुर्भावनापूर्ण प्रतिभागियों (potentially malicious participants) के कारण क्षति से बचाने के लिए आवश्यक हैं। जैसा कि प्रस्तावित है, PoX और स्टैकिंग प्रोटोकॉल के लिए आवश्यक है कि *इनाम सेट* को

निर्धारित करने के लिए स्टैक्स नोड एंकर ब्लॉक का उपयोग करने में सक्षम हो। यदि, दुर्घटना या दुर्भावना से, एंकर ब्लॉक से जुड़ा डेटा नोड्स के लिए अनुपलब्ध है, तो स्टैकिंग प्रोटोकॉल सामान्य रूप से काम नहीं कर सकता है - नोड्स यह नहीं जान सकते हैं कि क्या खनिक वैध ब्लॉक प्रतिबद्धताओं (valid block commitments) को प्रस्तुत कर रहा है या नहीं। F के लिए एक उच्च सीमा सुनिश्चित करता है कि स्टैक्स खनन शक्ति (Stacks mining power) का एक बड़ा हिस्सा एंकर ब्लॉक से जुड़े डेटा की प्राप्ति की पुष्टि (confirmation) करता है।

लापता डेटा से उगाही (Recovery from Missing Data)

अगर ऐसा होता है कि एक दुर्भावनापूर्ण माइनर (malicious miner) एक छिपे हुए या अमान्य ब्लॉक को एंकर ब्लॉक के रूप में स्वीकार करने में सक्षम है, स्टैक्स के नोड्स ऑपरेशन जारी रखने में सक्षम होना चाहिए। ऐसा करने के लिए स्टैक्स के नोड्स गायब एंकर ब्लॉक डेटा का मानना ऐसा करते हैं जैसे कि कोई एंकर ब्लॉक इनाम चक्र के लिए नहीं चुना गया था - इसलिए वैध चुनाव प्रतिबद्धताओं (valid election commitments) केवल *बर्न* होगा (जिसका अर्थ है PoB)। यदि एंकर ब्लॉक डेटा जो पहले गायब था वह स्टैक्स नोड को पता चला है, तो उस एंकर ब्लॉक के संबद्ध इनाम चक्र के लिए सभी नेता चुनावों (leader elections) को फिर से करना होगा, क्योंकि अब कई प्रतिबद्धताएं (commitments) हो सकती हैं जो पहले अमान्य थीं जो अब मान्य हैं।

फिर से नेता चुनाव कम्प्यूटेशनल रूप से महंगा होता है, और स्टैक्स श्रृंखला (Stacks chain) के एक बड़े पुनर्गठन (reorganization) में परिणाम होगा। हालाँकि, इस तरह के चुनाव पुनर्प्रसंस्करण (election reprocessing) केवल एक बार प्रति इनाम विंडो के लिए हो सकते हैं (केवल एक मान्य एंकर ब्लॉक इनाम चक्र के लिए मौजूद हो सकता है, चाहे वह छिपा हो या नहीं)। स्वाभाविक रूप से, जानबूझकर इस तरह के हमले को करने के लिए स्टैक्स माइनिंग पावर के एक बड़े अंश `F` के बीच मिलीभगत की आवश्यकता होगी - क्योंकि इस तरह के एक छिपे हुए ब्लॉक की पुष्टि (confirmation) बाद के `w*F` ब्लॉकों द्वारा की जानी चाहिए। अगर स्टैक्स माइनिंग पावर के इतने बड़े हिस्से के बीच मिलीभगत संभव है, तो हम मानते हैं कि एंकर ब्लॉक पर हमला करने से परे स्टैक्स श्रृंखला की सुरक्षा अन्य तरीकों से छेड़छाड़ की जाएगी।

स्टेकर समर्थन के साथ एंकरिंग (Anchoring with Stacker Support)

स्टेकर समर्थन लेनदेन के माध्यम से एंकर ब्लॉक चयन की सुरक्षा बढ़ जाता है। इस प्रोटोकॉल में, जब स्टैकिंग प्रतिभागी अपने हस्ताक्षरित भागीदारी संदेशों (signed participation messages) को प्रसारित करते हैं, तो वे एंकर ब्लॉकों के समर्थन का संकेत देते हैं। यह श्रृंखला टिप के हैश (chain tip's hash) द्वारा निर्दिष्ट किया गया है, और समर्थन संकेत तब तक मान्य है जब तक संदेश स्वयं मान्य है। यह एंकर ब्लॉक चयन पर एक अतिरिक्त आवश्यकता रखता है। एक एंकर ब्लॉक को एक निश्चित संख्या में माइनर पुष्टिकरण (miner confirmations) तक पहुंचने के अलावा, इसे वैध स्टेकर समर्थन

संदेश संकेतों (Stacker support message signals) के कुछ सीमा t को भी उत्तीर्ण करना होगा। यह एंकर ब्लॉक के हमले पर एक अतिरिक्त बोझ डालता है - न केवल हमलावर को खनन शक्ति के एक बड़े अंश के बीच मिलीभगत की आवश्यकता होगी, बल्कि उन्हें अपने ब्लॉक के अधिकांश स्टैकिंग प्रतिभागियों के बीच भी सांठ-गांठ करना होगा।

स्टेकर प्रत्यायोजन (Stacker Delegation)

प्रत्यायोजन की प्रक्रिया एक स्टैक्स वॉलेट एड्रेस (प्रतिनिधित्व पता - the represented address) को यह अनुमति देता है की वो अन्य पते (प्रतिनिधि / नुमायंदा पते - the delegate address) को नामित करे स्टैक प्रोटोकॉल में भाग लेने के लिए। यह प्रतिनिधि पता, जब तक प्रत्यायोजन मान्य है, तब तक स्टैकिंग संदेशों (अर्थात, संदेश जो स्टैक्स को लॉक करते हैं, बिटकॉइन इनाम पते को नामित करते हैं, और श्रृंखला टिप के लिए समर्थन का संकेत करते हैं) पर हस्ताक्षर करने और प्रसारित करने में सक्षम है प्रतिनिधित्व किए गए पते की ओर से। यह श्रृंखला टिप के लिए प्रतिनिधि पते (delegate address) अपने समर्थन सिग्नल के द्वारा नेटवर्क की सुरक्षा में योगदान करने के लिए प्रतिनिधित्व पते (represented address) के मालिक को अनुमति देता है। यह खनिकों द्वारा ब्लॉकचेन स्थिरता पर संभावित हमलों का मुकाबला करता है जैसे की छिपे हुए कांटे (hidden forks) की खनन की कोशिश, अवैध कांटे (invalid forks) छिपाना , और अन्य प्रकार के खनन दुर्व्यवहार (miner misbehavior)। सहायक प्रत्यायोजन स्टैक्स ब्लॉकचेन में दो नए लेनदेन प्रकार जोड़ता है:

- **प्रतिनिधि / नुमायंदा निधि** (Delegate Funds)। यह लेनदेन एक प्रतिनिधित्व-प्रतिनिधि (represented-delegate) संबंध शुरू करता है। यह निम्नलिखित डेटा वहन करता है:
    - प्रतिनिधि / नुमायंदा का पता (Delegate address)
    - एंड ब्लॉक (End Block): 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 करता है।
    - प्रत्यायोजित राशि (Delegated Amount): इस पते से STX की कुल राशि जिस की ओर से प्रतिनिधि पते (delegate address) स्टैकिंग संदेश जारी करने में सक्षम होगी।
    - रिवार्ड एड्रेस (*वैकल्पिक* - optional): एक बिटकॉइन पता जिसे प्रतिनिधि के स्टैकिंग संदेशों (delegate's Stacking messages) में धन प्राप्तकर्ता के रूप में निर्दिष्ट किया जाना चाहिए। यदि अनिर्दिष्ट है, तो प्रतिनिधि / नुमायंदा (delegate) यह पता चुन सकता है।
- **प्रत्यायोजन समाप्ति** (Terminate Delegation)। यह लेनदेन एक प्रतिनिधित्व-प्रतिनिधि संबंध को समाप्त करता है। यह निम्नलिखित डेटा वहन करता है:
    - प्रतिनिधि / नुमायंदा का पता (Delegate address)

ध्यान दें: किसी दिए गए प्रतिनिधित्व पते और प्रतिनिधि पते के बीच केवल एक ही सक्रिय प्रतिनिधित्व-प्रतिनिधि संबंध है (यानी, (*प्रतिनिधित्व-पता, प्रतिनिधि-पता*) जोड़ी विशिष्ट रूप से एक रिश्ते की

पहचान करता है)। यदि एक प्रतिनिधित्व-प्रतिनिधि संबंध अभी भी सक्रिय है और प्रतिनिधित्व पता एक नया "प्रतिनिधि निधि" लेनदेन ("delegate funds" transaction) को संकेत और प्रसारित करता है, तो नए लेनदेन की जानकारी पूर्व संबंध (relationship) को बदल देती है।

दोनों प्रकार के प्रतिनिधि लेनदेन (delegation transactions) का प्रतिनिधित्व पते (represented address) द्वारा हस्ताक्षरित होना चाहिए। ये स्टैक्स ब्लॉकचेन पर लेन-देन हैं, और स्टैक्स 2.0 जीनसिस ब्लॉक (Stacks 2.0 genesis block) के दौरान ब्लॉकचेन में लोड किए गए एक नेटिव स्मार्ट कांट्रॅक्ट के माध्यम से लागू किया जाएगा। इसलिए ये लेन-देन, अनुबंध-कॉल आह्वान (`contract-call` invocations) हैं। आह्वान किए गए तरीके निम्नलिखित द्वारा पहरा दिया गया हैं:

```
(asserts! (is-eq contract-caller tx-sender) (err u0))
```

यह सुनिश्चित करता है कि यह तरीकों को केवल प्रत्यक्ष लेनदेन निष्पादन (direct transaction execution) द्वारा लागू किया जा सकता है।

प्रत्यायोजन (delegation) के संदर्भ (context) में स्टैकिंग संदेशों का मूल्यांकन। यह निर्धारित करने के लिए कि स्टैकिंग संदेश द्वारा कौन से पतों की STX को लॉक किया जाना चाहिए, इस स्टैकिंग संदेश में प्रतिनिधित्व पता (represented address) शामिल होना चाहिए। इसलिए, यदि एक स्टैक्स पता कई प्रतिनिधित्व किए गए स्टैक्स पते के लिए प्रतिनिधि (delegate) है, तो प्रतिनिधि पते (delegate address) को प्रतिनिधित्व किए गए प्रत्येक पते के लिए एक स्टैकिंग संदेश प्रसारित करना चाहिए।

स्टैकिंग में खान समेकन का समाधान करना (Addressing Miner Consolidation in Stacking)

स्टैकिंग पुरस्कारों के लिए उपयोग किया जाने वाला PoX खनन समेकन (miner consolidation) को जन्म दे सकता है। क्योंकि जो खनिक स्टेकर के रूप में भी भाग लेते हैं वो दूसरे खनिकों (जो स्टेकर के रूप में भाग नहीं लेते हैं) पर अधिक लाभ प्राप्त कर सकते हैं, खनिकों स्टैक्स खरीदके इसका उपयोग करके अन्य खनिकों को बाहर निकालने के लिए प्रोत्साहित होंगे। चरम मामले में, यह समेकन खनन के केंद्रीकरण (centralization of mining) का कारण बन सकता है, जो स्टैक्स ब्लॉकचेन के विकेंद्रीकरण लक्ष्यों को कम करेगा। जब तक की हम सक्रिय रूप से इस संभावित समेकन को संबोधित करने के लिए अतिरिक्त तंत्र की जांच कर रहे हैं, जब तक हम समयबद्ध PoX तंत्र (time-bounded PoX mechanism) और एक स्टेकर-चालित तंत्र (Stacker-driven mechanism) का प्रस्ताव देते हैं।

समयबद्ध PoX (Time-Bounded PoX)। स्टैकिंग पुरस्कार माइनर समेकन को प्रोत्साहित करते हैं यदि खनिक नए क्रिप्टोक्यूरेंसी प्राप्त करने के लिए *स्थायी* लाभ (permanent advantages) प्राप्त करते हैं। हालाँकि, PoX की समयावधि (time period) को सीमित करके, यह लाभ समय के साथ कम हो जाता है। ऐसा करने के लिए, हम PoX के लिए दो समय अवधि निर्धारित करते हैं:

1. **पहला भाग** (Initial Phase)। इस चरण में, स्टैकिंग पुरस्कार ऊपर वर्णित रूप से आगे बढ़ते हैं - प्रतिबद्धता धन (commitment funds) स्टैकिंग पुरस्कार पते पर भेजे जाते हैं, सिवाय इसके कि यदि कोई खनिक एंकर ब्लॉक के वंशज (descendant of the anchor block) का खनन नहीं कर रहा है, या यदि किसी दिए गए इनाम चक्र के लिए पंजीकृत इनाम के पते (registered reward addresses) सभी समाप्त हो गए हैं । यह चरण लगभग 2 साल (100,000 बिटकॉइन ब्लॉक) तक चलेगा।
2. **सूर्यास्त / अंतिम भाग** (Sunset Phase)। पहला भाग के बाद, एक सूर्यास्त ब्लॉक (sunset block) निर्धारित किया जाता है। सूर्यास्त भाग शुरू होने के ~8 साल (400,000 बिटकॉइन ब्लॉक) बाद यह सूर्यास्त ब्लॉक होगा। सूर्यास्त ब्लॉक के बाद, इनाम के पते पर स्थानांतरित करने के बजाय, *सभी* खान की प्रतिबद्धताओं (miner commitments) को जला दिया जाना चाहिए। सूर्यास्त भाग के दौरान, इनाम / बर्न अनुपात प्रत्येक इनाम चक्र पर `0.25%` (1/400) से कम हो जाता है, ताकि 200 वें इनाम चक्र में, इनाम के पते पर ट्रांसफर किए गए धन और जला दिया गया धन का अनुपात `0.5` के बराबर होना चाहिए। । उदाहरण के लिए, यदि कोई माइनर 10 BTC प्रतिबद्ध (commit) करता है, तो माइनर को 5 BTC को इनाम के पते और 5 BTC को जले हुए पते (burn address) पर भेजना होगा।

PoX तंत्र (PoX mechanism) को समयबद्ध (time-bounding) करके, हम स्टैकिंग प्रोटोकॉल को अनुमति देते हैं की PoX का मदद से मौजूदा संसाधन से यह नए ब्लॉकचैन का समर्थन करे, और शुरुआत से ही खनिक और धारक (miners and holders) को नेटवर्क में भाग लेने के लिए प्रोत्साहन प्रदान करे। फिर ब्लॉकचेन के लिए प्राकृतिक उपयोग (natural use cases) जैसे विकसित होने लगेंगे, PoX प्रणाली धीरे-धीरे (PoX system) नीचे पैमाने पर (gradually scale down) हो सकती है।

स्टेकर चालित PoX (Stacker-driven PoX)। समेकन (consolidation) से खनिकों को और हतोत्साहित करने के लिए, तरल (liquid) STX टोकन (यानी गैर-स्टैक्ड - non-Stacked) के धारक अगले आगामी इनाम चक्र में PoX को निष्क्रिय करने के लिए मतदान (vote) कर सकते हैं। यह STX की किसी भी राशि (amount) के साथ किया जा सकता है, और PoX को निष्क्रिय करने के लिए मतदान का कार्य टोकन को लॉक नहीं करता है।

यह सतर्क उपयोगकर्ताओं के एक समुदाय (community of vigilant users) को विषयानुसार आधार पर समेकन से उत्पन्न होने वाले बुरे खनन व्यवहार से श्रृंखला की रक्षा करता है। विशेष रूप से, अगर तरल STX टोकन का एक अंश R, PoX को निष्क्रिय करने के लिए वोट करता है, तो यह केवल अगले इनाम चक्र के लिए अक्षम होता है। PoX को लगातार निष्क्रिय करने के लिए, STX धारकों को इसे निष्क्रिय करने के लिए लगातार वोट देना चाहिए।

शेष सतर्कता की लागत के कारण, यह प्रस्ताव $R = 0.25$ की सिफारिश करता है। इस लेखन के समय, यह किसी एकल STX आवंटन (allocation) से अधिक है, लेकिन इतना अधिक नहीं है कि खनन कार्टेल (mining cartel) को रोकने के लिए बड़े पैमाने पर सहयोग की आवश्यकता हो।

बिटकॉइन वायर प्रारूप (Bitcoin Wire Formats)

स्टैक्स ब्लॉकचैन में PoX का समर्थन करने के लिए नेता ब्लॉक प्रतिबद्धताओं (leader block commitments) के लिए तार प्रारूप (wire format) में संशोधन, और burnchain PoX भागीदारी के लिए नए तार स्वरूपों (new wire formats) की शुरूआत (जैसे, burnchain पर STX लॉकअप करना) की आवश्यकता होती है ।

नेता ब्लॉक प्रतिबद्धताओं (Leader Block Commits)

PoX के लिए, लीडर ब्लॉक कमिटमेंट PoB ब्लॉक कमिट्स के समान हैं: BTC ट्रांजेक्शन के इनपुट्स पर बाधाएं समान हैं, और `OP_RETURN` आउटपुट समान है। हालाँकि, *बर्न आउटपुट* अब पहले जैसा नहीं है। PoX के लिए, दूसरे से nth आउटपुट पर निम्नलिखित बाधाओं का लागू किया जाता है:

1. यदि ब्लॉक प्रतिबद्धता (block commitment) एक चुने हुए एंकर ब्लॉक के साथ एक इनाम चक्र में है, और यह ब्लॉक प्रतिबद्धता PoX एंकर ब्लॉक के वंशज (या उसी एंकर ब्लॉक) का निर्माण करती है, तो प्रतिबद्धता को मौजूदा ब्लॉक के लिए चुने गए PoX प्राप्तकर्ताओं (chosen PoX recipients) का उपयोग करना चाहिए। । a. PoX प्राप्तकर्ताओं को "स्टैकिंग सर्वसम्मति एल्गोरिथ्म" ("Stacking Consensus Algorithm") में वर्णित के रूप में चुना जाता है: पते को प्रतिस्थापन (replacement) के बिना चुना जाता है, पिछले बर्न ब्लॉक के सॉर्टिंग हैश (sortition hash) का उपयोग करके, यह मिश्रित होता है पिछले बर्न ब्लॉक बर्न हेडर हैश बीज के रूप में (previous burn block's burn header hash as the seed) जब ChaCha12 कूट-यादृच्छिक फ़ंक्शन (ChaCha12 pseudorandom function) में इस्तेमाल होता है M पते का चयन करने के लिए। b. बी लीडर ब्लॉक कमिट ट्रांजेक्शन को चयनित M पतों को आउटपुट [1, M] के रूप में उपयोग करना चाहिए, मतलब कि, दूसरे से (M+1)वें आउटपुट के माध्यम से चुनिंदा PoX पतों के अनुरूप (correspond) है। इन पतों का क्रम मायने नहीं रखता। इनमें से प्रत्येक आउटपुट को BTC की समान मात्रा प्राप्त होनी चाहिए। c. यदि इनाम सेट N में शेष पतों (remaining addresses) की संख्या M से कम है, तो नेता ब्लॉक प्रतिबद्धता लेन-देन (leader block commit transaction) BTC को जला देना चाहिए (M-N) बर्न आउटपुट को शामिल करके।
2. अन्यथा, दूसरे से (M+1)वें आउटपुट के पते बर्न पते (burn addresses) होने चाहिए, और इन आउटपुट द्वारा जलाई गई राशि को ब्लॉक कमिट द्वारा की गई प्रतिबद्ध राशि (amount committed) के रूप में गिना जाएगा।

इसके अलावा, सूर्यास्त चरण के दौरान (यानी, श्रृंखला में 100,000 और 500,000 वें बर्न ब्लॉक के बीच), खनिक को *सूर्यास्त बर्न* आउटपुट (sunset burn output) शामिल करना चाहिए। यह एक M+1

अनुक्रमित (indexed) आउटपुट है जिसमें सूर्यास्त बर्न अनुपात (sunset burn ratio) को पूरा करने के लिए आवश्यक बर्न राशि शामिल है, और इसे बर्न अड्रेस में भेजा जाना चाहिए:

sunset_burn_amount = (total_block_commit_amount) * (reward_cycle_start_height - 100,000) / (400,000)

जहां total_block_commit_amount बराबर है [1, M+1] आउटपुट के योग के.

सूर्यास्त चरण (sunset phase) समाप्त होने के बाद (यानी, ब्लॉक >= 500,000 वां बर्न ब्लॉक), ब्लॉक कमिट्स *केवल* बर्न होते हैं, इंडेक्स 1 पर एक बर्न आउटपुट के साथ।

बिटकॉइन पर STX संचालन (STX Operations on Bitcoin)

जैसा कि ऊपर वर्णित है, PoX स्टैकर्स को बिटकॉइन के साथ-साथ स्टैक्स ब्लॉकचेन पर `stack-STX` संचालन प्रस्तुत (submit `stack-stx` operations) करने देता है। स्टैक्स श्रृंखला भी पते को बिटकॉइन श्रृंखला पर STX हस्तांतरण प्रस्तुत (submit STX transfers) करने देती है। इस तरह के ऑपरेशन का मूल्यांकन केवल उस बर्न ब्लॉक में चुने गए एंकर ब्लॉक के खनिक द्वारा किया जाता है जो ऑपरेशन को शामिल करने वाले बर्न ब्लॉक का तुरंत अनुसरण करता है। उदाहरण के लिए, अगर Burnchain ब्लॉक 100 में एक `TransferStxOp` होता है, तो Burnchain ब्लॉक 101 द्वारा चुने गए स्टैक्स ब्लॉक उस हस्तांतरण (transfer) को संसाधित (process) करेगा। बिटकॉइन श्रृंखला पर जमा करने के लिए, स्टैकर्स को दो बिटकॉइन लेनदेन (transactions) प्रस्तुत (submit) करने होंगे:

- PreStxOp: यह ऑपरेशन बाद के `StackStxOp` या `TransferStxOp` को मान्य (validate) करने के लिए स्टैक्स ब्लॉकचेन नोड को तैयार करता है।
- StackStxOp: यह ऑपरेशन `stack-stx` ऑपरेशन को निष्पादित (executes) करता है।
- TransferStxOp: यह ऑपरेशन प्रेषक से प्राप्तकर्ता (sender to a recipient) को STX स्थानांतरित करता है

उपरोक्त परिचालनों (operations) के तार प्रारूप (wire formats) निम्नानुसार हैं:

PreStxOp

इस ऑपरेशन में उस पहले Bitcoin आउटपुट के लिए एक OP_RETURN आउटपुट शामिल है जो इस प्रकार दिखता है:

```
0     2  3
|------|--|
 magic  op
```

जहाँ op = p (ascii encoded).

फिर, दूसरा बीटकोइन आउटपुट स्टेकर एड्रेस *होना चाहिए* जो कि `StackStxOp` में उपयोग किया जाएगा। यह पता एक मानक पता प्रकार (standard address type) होना चाहिए जो स्टैक्स-ब्लॉकचैन नोड द्वारा पार्स करने योग्य हो (parseable)।

StackStxOp

बीटकोइन ऑपरेशन के लिए पहला इनपुट उस UTXO का उपभोग करना *चाहिए* जो कि `PreStxOp` का दूसरा आउटपुट है। यह पुष्टि करता है कि `StackStxOp` उपयुक्त स्टेकर पते द्वारा हस्ताक्षरित था।

इस ऑपरेशन में पहले बीटकोइन आउटपुट के लिए एक OP_RETURN आउटपुट शामिल है:

```
0     2  3                          19       20
|------|--|----------------------------|---------|
 magic  op         uSTX to lock (u128)     cycles (u8)
```

जहाँ op = x (ascii encoded).

जहां अहस्ताक्षरित पूर्णांक (unsigned integer) बड़ा-एंडियन (big-endian) एन्कोडेड है।

दूसरा बिटकॉइन आउटपुट किसी भी स्टैकिंग रिवार्ड के लिए रिवार्ड एड्रेस के रूप में उपयोग किया जाएगा।

TransferStxOp

बीटकोइन ऑपरेशन के लिए पहला इनपुट उस UTXO का उपभोग करना *चाहिए* जो कि PreStxOp का दूसरा आउटपुट है। यह पुष्टि करता है कि TransferStxOp उचित STX पते द्वारा हस्ताक्षरित था।

इस ऑपरेशन में पहले बीटकोइन आउटपुट के लिए एक OP_RETURN आउटपुट शामिल है:

```
0     2  3                          19       80
|------|--|----------------------------|---------|
 magic  op      uSTX to transfer (u128)     memo (up to 61 bytes)
```

जहाँ op = $ (ascii encoded).

जहां अहस्ताक्षरित पूर्णांक (unsigned integer) बड़ा-एंडियन (big-endian) एन्कोडेड है।

दूसरा बिटकॉइन आउटपुट या तो p2pkh या p2sh आउटपुट है ताकि प्राप्तकर्ता स्टैक्स का पता (recipient Stacks address) इसी की 20-बाइट हैश (hash160) से प्राप्त किया जा सकता है।

संबंधित कार्य (Related Work)

इस SIP के अनुसमर्थन (ratified) के बाद इस खंड का विस्तार किया जाएगा।

पिछेड़ी अनुकूलता (Backwards Compatibility)

लागू नहीं (Not applicable)।

सक्रियण (Activation)

कम से कम 20 खनिकों को स्टैक 1.0 में .miner नामस्थान (namespace) में नाम दर्ज करना चाहिए। एक बार 20 वें खनिक पंजीकृत (registered) होने के बाद, स्टैक 1.0 की स्थिति को स्नैपशॉट किया जाएगा। 300 बिटकॉइन ब्लॉक बाद में (बिटकॉइन ब्लॉक 666050), स्टैक्स 2.0 ब्लॉकचेन लॉन्च करेगा। स्टैक्स 2.0 इस SIP को लागू करता है।

संदर्भ कार्यान्वयन (Reference Implementations)

Rust में लागू किया गया। https://github.com/blockstack/stacks-blockchain देखिए।