प्रूफ-ऑफ़-प्रूफ:

एक विकेंद्रीकृत, भरोसेमंद, पारदर्शी, और स्केलेबल माध्यमों की विरासत

प्रूफ-ऑफ-वर्क सिक्योरिटी

VeriBlock, Inc.

Maxwell Sanchez
Justin Fisher

संस्करण 1.0p

संक्षेप

प्रूफ-ऑफ़-प्रूफ आम सहमति प्रोटोकॉल ब्लॉक चेन अन्य ब्लॉक चेन से सबूत के काम की सुरक्षा के वारिस करने के लिए सक्षम बनाता है, एक पारिस्थितिकी तंत्र बनाने जिसमें सुरक्षा बिटकॉइन की तरह स्थापित ब्लॉक श्रृंखला पर उत्पन्न होती है और अन्य ब्लॉक श्रृंखला के लिए फैली हुई है । इस तरह का पारिस्थितिकी तंत्र उद्देश्य-निर्मित श्रृंखलाओं के लिए सुरक्षा तंत्र के रूप में उपयोग करके बिटकॉइन की अप्रत्यक्ष दरिद्रता पैदा करता है । सभी ब्लॉक श्रृंखला बिटकॉइन के सुरक्षा के संदर्भ में संचालित करने के लिए सक्षम बनाता है जो एक पदानुक्रमित सुरक्षा मॉडल से लाभ, बंद श्रृंखला लेनदेन नेटवर्क और पक्ष-चेन सहित, दरिद्र के अन्य क्षेत्रों में वर्तमान प्रगति । हम बिटकॉइन खनिकों की भागीदारी या अनुमोदन के बिना, किसी भी केंद्रीकृत संस्थाओं या संयुक्त नोड्स के बिना इस विरासत के लिए एक साधन का प्रस्ताव है, और ब्लॉक चेन जो इस प्रोटोकॉल को अपनाने पर कोई तकनीकी सीमाओं पर थोपे बिना ।

1 परिचय

सबसे बड़ा ब्लॉक चेन आज का सामना करना पड़ मुद्दों में से एक-उनके तक पहुंचने और ब्लॉक श्रृंखला डेटा पर आम सहमति बनाए रखने की क्षमता-जटिलता और आगामी प्रौद्योगिकियों के एक व्यापक चयन की सुरक्षा पर बहस की एक किस्म छिड़ गया है ।

बिटकॉइन द्वारा इस्तेमाल किया प्रूफ-ऑफ़-वर्क प्रोटोकॉल दो प्राथमिक आलोचनाओं से मुलाकात की है: (1) बेकार बिजली की खपत, और (2) कम हैश शक्ति के साथ जंजीरों पर कमजोर । खपत बिजली में अक्षमता के बारे में आलोचना ठोस स्तर पर खड़ा है-तो भी एक प्रकाश बल्ब की रेशा सकता इसी तरह एक अकुशल कंडक्टर कहा जाता है, इसके प्रकाश का उत्पादन करने की क्षमता के बावजूद । यह सच है, तथापि, कि छोटे क्रिप्टो सबूत के काम को लागू करने मुद्राओं अपेक्षाकृत कम लागत वाले हमलों की चपेट में हैं, खासकर जब एक बड़ा एक ही हैश एल्गोरिथ्म का उपयोग श्रृंखला मौजूद है ।

इन आलोचनाओं के जवाब में, वैकल्पिक आम सहमति तंत्र की एक किस्म का प्रस्ताव किया गया है और सबूत के दांव सहित विकसित, जहां उपयोगकर्ताओं को मेरे लिए देशी टोकन में शेष पकड़,

व्यावहारिक बीजांटिन दोष सहिष्णुता और तरंग प्रोटोकॉल आम सहमति एल्गोरिथ्म जो बेड़ा और पासोस जैसे शास्त्रीय आम सहमति एल्गोरिदम के पीछे विचारों को बड़े पैमाने पर और भरोसेमंद सिस्टम पर कार्य करने के लिए अनुकूल है, और संयुक्त नोड्स या विश्वसनीय नोड्स जो नेटवर्क अधिकारियों के रूप में कार्य करते है और आम सहमति संघर्ष का समाधान ।

इन आम सहमति एल्गोरिदम के एक सबूत के लाभ के कुछ काम आम सहमति तंत्र से कुछ:-ऊष्मा ध्वनि सुरक्षा उंमीदें, भरोसेमंद और अनुमति खनिकों की कम भागीदारी, गणितीय-नेटवर्क के सत्यापन रिप्लायिंग नए नोड्स के लिए इतिहास, महत्वपूर्ण अवसर लागत पर हमला करने के लिए, आदि

हमारे सबूत के प्रूफ सहमति प्रोटोकॉल एक शक्तिशाली सबूत के काम ब्लॉक श्रृंखला के हैश शक्ति रिसाइकिलिंग द्वारा इन चिंताओं के दोनों पते को अतिरिक्त ब्लॉक श्रृंखला के एक असीमित मात्रा में सुरक्षित ।

2 पिछले प्रौद्योगिकियों

मौजूदा उच्च सुरक्षा ब्लॉक चेन की सुरक्षा का पुन: उपयोग करने के लिए पिछले प्रयास किए गए हैं । 2011 में नेमकॉइन सहित कई ब्लॉक श्रृंखला, अपनाया विलय खनन और AuxPoW प्रोटोकॉल, जो बिटकॉइन खनिक एक साथ ही दोनों बिटकॉइन और एक या एक से अधिक सहायक ब्लॉक चेन की अनुमति दी । 2013 में, मास्टरकॉइन (अब ओमनी/ ओम्नीलेयर) बिटकॉइन ब्लॉक श्रृंखला में डेटा embedding द्वारा बिटकॉइन के शीर्ष पर चलाता है, जो एक प्रोटोकॉल का शुभारंभ किया ।

2.1 विलय खनन (AuxPoW)

विलय खनन एक या एक से अधिक सहायक ब्लॉक चेन पर एक साथ मेरा करने के लिए एक माता पिता के ब्लॉक श्रृंखला की खान में सक्षम बनाता है । AuxPoW का उपयोग कर मेरा मर्ज करने के लिए अन्य ब्लॉक चेन की अनुमति देने के लिए पैरेंट ब्लॉक चेन ही कोई संशोधन की आवश्यकता है । मेरा विलय करने के लिए, एक खान में काम करनेवाला पहले वैध ब्लॉक (ओं) के लिए सहायक ब्लॉक श्रृंखला (ओं) का निर्माण करना चाहिए, और फिर जनक ब्लॉक श्रृंखला में इन ब्लॉकों के कुछ सबूत शामिल है जो वे मेरा प्रयास (अक्सर जनक ब्लॉक सिक्का आधार में सहायक ब्लॉक श्रृंखला हैश द्वारा लेनदेन) । अगर एक खान में काम करता है सफलतापूर्वक एक लक्ष्य है कि एक या एक से अधिक संतुष्ट मर्ज-खनन या माता-पिता की ब्लॉक श्रृंखला, इसी ब्लॉक (ओं) और सबूत के काम समाधान संयुक्त और उनके संबंधित ब्लॉक श्रृंखला (ओं) के नीचे के सबूत का हल ।

विलय-खनन माता-पिता ब्लॉक चेन खनिक की सक्रिय भागीदारी की आवश्यकता है, और हैश दर जो सहायक ब्लॉक श्रृंखला वारिस के प्रतिशत माता पिता के ब्लॉक श्रृंखला की हैश शक्ति है जो विशेष रूप से विलय-खनन प्रदर्शन कर रहा है का प्रतिशत है सहायक ब्लॉक चेन ।

विलय खनन प्रभावी पैमाने पर सहायक ब्लॉक चेन की एक बड़ी संख्या को सुरक्षित करने के लिए नहीं है, क्योंकि यह है कि माता पिता के ब्लॉक श्रृंखला खनिक ट्रैक की आवश्यकता होती है और सहायक ब्लॉक श्रृंखला की एक बड़ी मात्रा के लिए ब्लॉक इकट्ठा । यह भी सहायक ब्लॉक जंजीरों बलों के जनक ब्लॉक श्रृंखला के रूप में एक ही हैश एल्गोरिथ्म का उपयोग करने के लिए । अंत में, कार्यांवयन के अधिकांश में, माता पिता के ब्लॉक श्रृंखला खनिक सहायक ब्लॉक श्रृंखला पर हमला करने के लिए अवसर लागत केवल विलय की लागत सहायक ब्लॉक श्रृंखला वैध रूप से खनन नहीं है, के रूप में खान में काम करने के लिए जारी रख सकते है माता पिता के ब्लॉक श्रृंखला (और विलय-मेरा अंय ब्लॉक श्रृंखला) ईमानदारी से जबकि एक और सहायक नेटवर्क पर हमले का प्रयास ।

2.2 स्तरित प्रौद्योगिकियों

ब्लॉक चेन या छद्म ब्लॉक चेन एक और ब्लॉक श्रृंखला के भीतर अपने ब्लॉक श्रृंखला के पूर्ण या निकट संपूर्णता लेखन द्वारा अत्यधिक सुरक्षित ब्लॉक चेन की सुरक्षा का वारिस । "एन्हांस्ड" या "जानकारी" इन तकनीकों के लिए क्लाइंट पेरेंट ब्लॉक चेन नेटवर्क पर नोड्स के रूप में कार्य और एम्बेडेड डेटा जो उनके ब्लॉक श्रृंखला के लिए विशेष अर्थ है के लिए देखें । इन डेटा तो माध्यमिक या एंबेडेड ब्लॉक श्रृंखला के जोड़तोड़ प्रदर्शन करने के लिए अपने स्वयं के नियमों के तहत व्याख्या कर रहे हैं । स्तरित प्रौद्योगिकियों के कार्यांवयन के कुछ: ओमनी/ओमनी परत (पूर्व मास्टरकॉइन), रंगीन सिक्के, और प्रतिपक्ष ।

द्वितीयक/एंबेडेड ब्लॉक श्रृंखला पर पुनर्संगठनों में पैरेंट ब्लॉक श्रृंखला परिणाम में पुनर्गठन । सामांयतया, जब कोई हस्तांतरण पर द्वितीयक/एम्बेडेड खंड श्रृंखला बनाया है, तो पैरेंट ब्लॉक श्रृंखला पर कोई हस्तांतरण बनाया है । इस ट्रांसक्शनल डेटा या एक प्रतिनिधित्व (हैश) तत्संबंधी OP_RETURN और "असंभव" पते जो डेटा एंबेड और एक ज्ञात इसी सार्वजनिक/निजी कुंजी जोड़ी नहीं है सहित साधन की एक किस्म का उपयोग कर माता पिता के ब्लॉक श्रृंखला लेनदेन में एंबेडेड है ।

एक माता पिता के ब्लॉक श्रृंखला के भीतर एक माध्यमिक ब्लॉक श्रृंखला ब्लॉक-समय सीमा और न्यूनतम भंडारण क्षमता सहित माध्यमिक ब्लॉक श्रृंखला पर महत्वपूर्ण सीमाएं लगाता है । दक्षता के लिए, यह अक्सर माध्यमिक ब्लॉक श्रृंखला की आवश्यकता के लिए पता प्रारूप (और इसी हस्ताक्षर एल्गोरिथ्म) के जनक ब्लॉक श्रृंखला का उपयोग । द्वितीयक ब्लॉक श्रृंखला के उपयोगकर्ताओं को भी स्वयं और द्वितीयक ब्लॉक श्रृंखला पर लेन-देन करने के लिए पैरेंट ब्लॉक श्रृंखला पर टोकन खर्च करना होगा । अंत में, इन तकनीकों में महत्वपूर्ण कठिनाई वॉल्यूम (हस्तांतरण की संख्या में मापा, नहीं आवश्यक हस्तांतरण का आकार) पैरेंट ब्लॉक श्रृंखला द्वारा समर्थित स्केलिंग से बाहर है । जबकि ओमनी (परत) की दुकान और हस्तांतरण संचारित "संलग्नक" एक धार नेटवर्क पर की तरह प्रौद्योगिकियों, ब्लॉक श्रृंखला पर एक अद्वितीय लेनदेन एक सौदे की आवश्यकता है बिट सिक्का पर प्रसारण के रूप में अच्छी तरह से ।

2.3 चैनडीबी

बिटकॉइन के लिए एक श्रृंखला हासिल करने के लिए चैनडीबी प्रस्ताव की आवश्यकता है कि चैनडीबी ब्लॉक-निर्माण नोड्स एक बिटकॉइन लेनदेन का निर्माण करने के लिए सहयोग करें जो अगले चैनडीबी ब्लॉक को नोट करता है, बिटकॉइन के ब्लॉक समय के लिए सुरक्षित श्रृंखला के न्यूनतम ब्लॉक समय की आवश्यकता है, कि पूरी तरह से मांय चैनडीबी नोड्स भी पूरी तरह से मांय बिटकॉइन नोड्स (हालांकि एक मॉडल चैनडीबी श्रृंखला में एम्बेडेड बिटकॉइन के ज्ञान की तरह का उपयोग कर के रूप में अच्छी तरह से कार्य करने के लिए प्रकट होता है), और बन गया एक हमले वेक्टर जिसमें बिटकॉइन खनिक द्वारा भुगतान शुल्क ले वैध चैनडीबी बोली लगाने, लेकिन अभी भी एक वैकल्पिक चैनडीबी ब्लॉक सहित द्वारा चैनडीबी ब्लॉक श्रृंखला नियंत्रण-एक अविश्वसनीय रूप से बड़े शुल्क के साथ लेनदेन को परिभाषित । इसके अतिरिक्त, एक हमलावर जो एक चैनडीबी ब्लॉक श्रृंखला को संशोधित करने के लिए इच्छा केवल शुल्क है कि हर एक कुछ बार चैनडीबी ब्लॉक के ब्लॉक इनाम से अधिक चैनडीबी ब्लॉक श्रृंखला पर एक बहु ब्लॉक पुनर्लेखन का एक महत्वपूर्ण मौका है भुगतान करने की आवश्यकता होगी; एक चैनडीबी ब्लॉक श्रृंखला संभावित सुरक्षा आईएसएस होता.. ।

2.4 मौजूदा प्रौद्योगिकियों का सारांश

सहायक/माध्यमिक ब्लॉक चेन पर एक माता पिता के ब्लॉक श्रृंखला के सबूत का काम सुरक्षा का उपयोग करने के लिए मौजूदा प्रौद्योगिकियों सुरक्षा के स्तर के बारे में महत्वपूर्ण कमियां के साथ आता है, सीमाओं सहायक/ दरिद्रता की चिंता ।

3 लक्ष्य

प्रूफ-ऑफ़-प्रूफ एक सुरक्षा विरासत (SI) ब्लॉक श्रृंखला (एक मर्ज खनन सहायक ब्लॉक श्रृंखला या एक स्तरित प्रौद्योगिकी माध्यमिक ब्लॉक श्रृंखला के अनुरूप) एक सुरक्षा प्रदान (SP) ब्लॉक श्रृंखला की पूरी प्रूफ-ऑफ़-वर्क सुरक्षा वारिस करने के लिए सक्षम करने के लिए लक्ष्य (एक माता पिता के ब्लॉक श्रृंखला के अनुरूप) ।

यह विरासत एसआई ब्लॉक चेन पर किसी भी गैर तुच्छ सीमाओं थोपना नहीं चाहिए, सपा ब्लॉक चेन या ज्ञान की अनुमति की आवश्यकता नहीं होनी चाहिए/SP ब्लॉक चेन खनिकों की भागीदारी, किसी भी केंद्रीकृत नेटवर्क प्राधिकरण की आवश्यकता नहीं होनी चाहिए (सहित फ़ेडरेटेड नोड्स), और SP ब्लॉक चेन विफल रहता है जो घटना में SI ब्लॉक चेन गैर-कार्यशील नहीं छोड़ना चाहिए । इसके अतिरिक्त, SI ब्लॉक चेन नेटवर्क के गैर खनन उपयोगकर्ताओं को सपा ब्लॉक चेन नेटवर्क के साथ इंटरफेस करने के लिए नहीं होना चाहिए, न ही वे अपने मूल टोकन के किसी भी पकड़ करने के लिए आवश्यक होना चाहिए ।

4 पिओपि प्रोटोकॉल

पिओपि प्रोटोकॉल खान में काम करनेवाला है जो एक ब्लॉक श्रृंखला के वर्तमान राज्य के आवधिक प्रकाशनों एक और ब्लॉक श्रृंखला के लिए प्रदर्शन के एक नए प्रकार का परिचय । इन प्रकाशनों को संभावित ब्लॉक श्रृंखला पुनर्गठन की स्थिति में संदर्भित कर रहे हैं । पिओपि की आवश्यकता है एक ब्लॉक श्रृंखला जैसे कम-हैश दर स्थानीयPOW, POS, आदि के रूप में ब्लॉक, बनाने के कुछ मतलब है

4.1 परिभाषाएँ

सर्वसंमति वारिस (CI) ब्लॉक श्रृंखला: एक ब्लॉक श्रृंखला पिओपि, जो एक और ब्लॉक श्रृंखला से पिओडब्लू वारिस द्वारा सुरक्षित ।

सहमति प्रदान (CP) ब्लॉक श्रृंखला: एक स्थापित, उच्च सुरक्षा ब्लॉक श्रृंखला है जो एक एसआई ब्लॉक श्रृंखला से पिओडब्लू वारिस ।

ब्लॉक श्रृंखला राज्य डेटा: किसी ब्लॉक श्रृंखला की वर्तमान स्थिति के बारे में डेटा, जैसे कि नवीनतम ब्लॉक शीर्षलेख, ब्लॉक हैश, लेन-देन की मेर्कले रूट आदि ।

पिओपि सुरंगवाला: एक नए प्रकार की खान में काम करनेवाला जो एक एसआई ब्लॉक श्रृंखला से ब्लॉक श्रृंखला राज्य डेटा के प्रकाशनों एक सपा ब्लॉक श्रृंखला के लिए प्रदर्शन करता है ।

4.2 पिओपि खनन प्रक्रिया का अवलोकन

पिओपि खनिकों के रूप में सेवा संचार/ एक SI ब्लॉक चेन और एक सपा ब्लॉक श्रृंखला के बीच लेन-देन पुलों । के रूप में अक्सर के रूप में वे चाहते हैं, पिओपि खनिक SI ब्लॉक श्रृंखला से सबसे हाल ही में ब्लॉक श्रृंखला राज्य डेटा ले जाएगा और यह सपा ब्लॉक श्रृंखला के लिए, कुछ पहचानकर्ता है, जो उंहें बाद में एस के साथ एक सपा ब्लॉक श्रृंखला लेनदेन बनाने के द्वारा मुआवजा प्राप्त करने की अनुमति देता है के साथ प्रकाशित करें मैं श्रृंखला राज्य डेटा ब्लॉक और उस में एंबेडेड पहचानकर्ता, और यह सपा ब्लॉक श्रृंखला नेटवर्क को प्रस्तुत करता है । एक SP ब्लॉक श्रृंखला हस्तांतरण में ब्लॉक श्रृंखला स्थिति डेटा एंबेडिंग के लिए कई विभिंन विधियों का उपयोग किया जा सकता: OP_RETURN, नकली पते, मल्टीसिग में फर्जी पते, आदि । पिओपि खान में काम करता है तो लेनदेन के लिए प्रतीक्षा करता है एक सपा ब्लॉक श्रृंखला ब्लॉक में शामिल हो, प्रकाशन के सबूत के कुछ फार्म का निर्माण, उनके लिए आवश्यक किसी भी पहचान की जानकारी के लिए प्रकाशन के लिए ऋण लेने के लिए कहते हैं, और इस सबूत को वापस प्रस्तुत एसआई ब्लॉक एक विशेष पिओपि खनन लेनदेन के रूप में चेन ।

4.3 पिओपि प्रकाशन डेटा

आदेश में OP_RETURN का लाभ लेने के लिए, SI ब्लॉक चेन राज्य डेटा भुगतान के लिए माईनर की पहचान करने के कुछ साधनों के साथ साथ 80 बाइट्स के भीतर फिट करने की जरूरत है । यह अनुशंसा की जाती है कि SI ब्लॉक श्रृंखला के पूरे ब्लॉक शीर्षलेख को बाद में चर्चा किए गए सुरक्षा भेद्यता को बंद करने के लिए प्रकाशित किया जाए. पिछले ब्लॉक हैश और मेर्कले ट्री के लिए 194-bit हैश का उपयोग करके, मानक ब्लॉक हैडर एक संस्करण, पिछले ब्लॉक हैश, मेर्कले ट्री हैश, टाइमस्टैंप, एनबिट्स शैली लक्ष्य से मिलकर प्रारूप, और उपनाम केवल 64 बाइट्स के स्थान पर रह रहे हैं, सेशन के 16 बाइट्स छोड़ पिओपि खान पहचान के लिए OP_RETURN डेटा (जैसे कि खान के पते के पहले 16 बाइट्स) । जब पिओपि माईनर एसआई ब्लॉक श्रृंखला के लिए अपने पिओपि खनन लेनदेन प्रस्तुत, वे पूर्ण SI ब्लॉक श्रृंखला का पता है जिसकी पहली 16 बाइट्स में खान में पहचान के इन 16 बाइट्स मैच शामिल होंगे ।

4.4 पिओपि खनन लेनदेन

विशेष पिओपि खनन हस्तांतरण प्रदर्शित करता है कि SI ब्लॉक चेन स्थिति डेटा sp ब्लॉक चेन हस्तांतरण, जो एक sp ब्लॉक श्रृंखला ब्लॉक में शामिल किया गया था में शामिल किया गया था । इस तरह, यह एसआई ब्लॉक चेन राज्य डेटा जो मूल रूप से (खान में पहचान के साथ) प्रकाशित किया गया था शामिल करने की जरूरत है, सपा ब्लॉक श्रृंखला एसआई ब्लॉक चेन राज्य डेटा युक्त लेनदेन, मेर्कले पथ (या सबूत का एक और रूप ऐसे एक के लिए एक गवाह के रूप में क्रिप्टोग्राफ़िक संचयक, यदि sp ब्लॉक चेन लेन-देन के लिए एक मेर्कले ट्री के अलावा किसी अन्य संरचना का उपयोग करता है) जो एक sp ब्लॉक चेन ब्लॉक में लेन-देन का समावेश दर्शाता है, और ब्लॉक करने के लिए संगत sp ब्लॉक चेन ब्लॉक शीर्ष लेख जिसमें SI ब्लॉक श्रृंखला राज्य डेटा प्रकाशित किया गया था । इसके अतिरिक्त, खनन लेनदेन पूर्ण खान में पहचान प्रदान करने के लिए अगर यह प्रकाशित डेटा में अपनी संपूर्णता में शामिल नहीं किया गया है की जरूरत है (उदाहरण: पूरा पता जिसका पहला 16 बाइट्स एक ओ में प्रकाशित माईनर पहचान के 16 बाइट्स मैच.. ।

4.5 पिओपि खनन लेनदेन सत्यापन

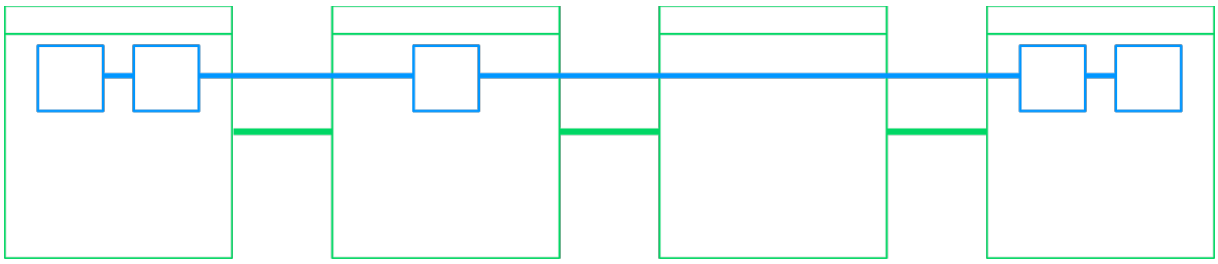
एसआई ब्लॉक चेन पर साथियों को प्रकाशित एसआई ब्लॉक श्रृंखला राज्य डेटा की वैधता की जांच द्वारा एक पिओपि खनन लेनदेन को मांय, प्रदान की सपा ब्लॉक चेन लेनदेन में शामिल किए जाने के लिए जांच, सपा ब्लॉक श्रृंखला लेनदेन सुनिश्चित प्रदान की सपा ब्लॉक श्रृंखला ब्लॉक है हैडर मेर्कले पेड़ (या सबूत के कुछ अंय रूप, ऐसे एक क्रिप्टोग्राफ़िक संचयक गवाह के रूप में मूल्यांकन), और सुनिश्चित करना है कि सपा ब्लॉक श्रृंखला के प्रदान की ब्लॉक शीर्षक (ओं) सपा ब्लॉक श्रृंखला पर "सबसे लंबे समय तक" पिओडब्लू श्रृंखला का निर्माण ।

एसआई ब्लॉक चेन राज्य डेटा की वैधता की जाँच केवल प्रकाशित राज्य डेटा के लिए संगत ब्लॉक के लिए एसआई ब्लॉक श्रृंखला में वापस देख की आवश्यकता है । प्रदान किए गए SP ब्लॉक श्रृंखला

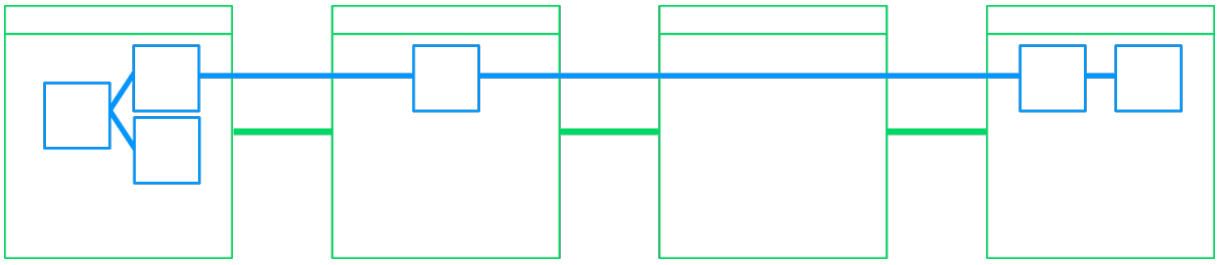
हस्तांतरण में शामिल करने के लिए जाँच कर रहा है हस्तांतरण पार्स कर रहा है और OP_RETURN के बाद डेटा की जाँच, या किसी एन्कोडेड प्रपत्र, जैसे मल्टीसिग पते के अंदर प्रकट करने के लिए ब्लॉक श्रृंखला स्थिति डेटा के लिए । उसके बाद, sp ब्लॉक चेन हस्तांतरण हैश किया गया है और मेर्कले पथ का अनुसरण किया जाता है, जो मेर्कले रूट में दिए गए SP ब्लॉक श्रृंखला शीर्ष लेख में एम्बेडेड परिणाम होना चाहिए । चूंकि केवल एक शुद्ध पिओडब्लू ब्लॉक श्रृंखला के शीर्ष लेख ब्लॉकों पर आम सहमति का निर्धारण करने के लिए पर्याप्त हैं, एसआई ब्लॉक चेन साथियों पर्याप्त जानकारी के लिए सुनिश्चित करें कि पिओपि प्रकाशन एक वैध सपा ब्लॉक श्रृंखला ब्लॉक में हुई ।

4.6 पिओपि ब्लॉक स्वरूप

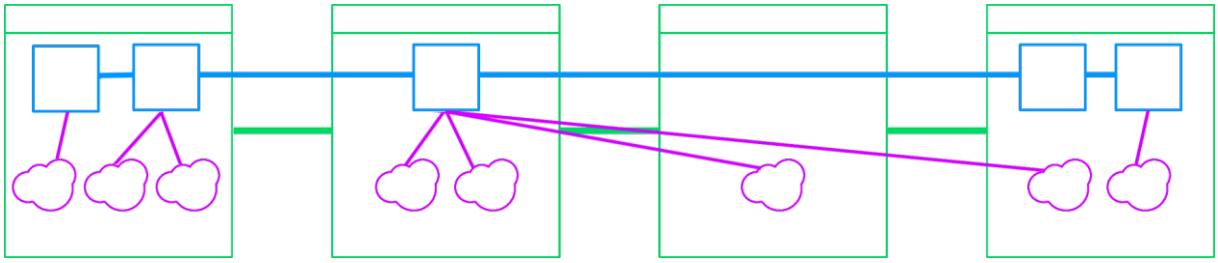
बाद में आम सहमति के लिए इस्तेमाल किया जा पिओपि खनन लेनदेन के लिए आदेश में, वे एसआई ब्लॉक श्रृंखला में संग्रहीत किया जाना चाहिए । इसके अतिरिक्त, सपा ब्लॉक श्रृंखला के ब्लॉक हेडर इस तरह से है कि सपा ब्लॉक श्रृंखला की आम सहमति साथियों की आवश्यकता के लिए सपा ब्लॉक श्रृंखला नेटवर्क के साथ इंटरफेस के बिना ट्रैक किया जा सकता है में संग्रहीत किया जाना चाहिए । इस तरह, एक ब्लॉक पिओपि को लागू करने की श्रृंखला पर ब्लॉक एक विशेष खंड के लिए नए सपा ब्लॉक चेन ब्लॉक हेडर पकड़ के बाद से पिछले एसआई ब्लॉक चेन ब्लॉक के सपा हेडर शामिल हैं ।



ऊपर चित्र में, ग्रीन ब्लॉक श्रृंखला एक एसआई ब्लॉक श्रृंखला पिओपि को लागू करने है । नीले ब्लॉकों सपा ब्लॉक श्रृंखला से हेडर हैं । एसआई ब्लॉक चेन में संग्रहित सपा ब्लॉक चेन हेडर को एक साथ जोड़कर पूरी सपा ब्लॉक चेन की पिओडब्लू बननी की पुष्टि की जा सकती है । घटना में है कि सपा ब्लॉक श्रृंखला पर एक कांटा होता है, एक एसआई ब्लॉक कई प्रतिस्पर्धी ब्लॉकों में शामिल कर सकते है और सपा ब्लॉक श्रृंखला हेडर भविष्य एसआई ब्लॉक श्रृंखला ब्लॉकों में एंबेडेड संघर्ष को हल करने की अनुमति:



प्रूफ-ऑफ़-प्रूफ खनन लेनदेन संदर्भ कर सकते हैं, सपा ब्लॉक चेन ब्लॉक जिसमें वे एसआई ब्लॉक चेन राज्य डेटा, किसी भी सपा ब्लॉक श्रृंखला ब्लॉक हेडर उनके संलग्न ब्लॉक या पिछले ब्लॉकों में (बैंगनी में पिओपि खनन लेनदेन) में संग्रहीत प्रकाशित के रूप में:



इस सुविधा के लिए ब्लॉक खनिकों (पिओडब्लू/ पिओएस/ आदि) पिओपि खनन लेनदेन द्वारा प्रदान की ब्लॉक हैडर डेटा ले लो, और पिओपि खनन लेनदेन वे अपने ब्लॉक में शामिल करना चाहते है के लिए संदर्भ प्रदान करने के लिए आवश्यक शून्य या अधिक सपा ब्लॉक श्रृंखला हेडर स्थापित करें ।

5 पिओपि के साथ फोर्क संकल्प

सभी प्रस्तावित कांटों के बीच "सर्वश्रेष्ठ" फोर्क एक संचई स्कोर के आधार पर चुना गया है । पिओपि में, तथापि, एक फोर्क का स्कोर एक और फोर्क के सापेक्ष गणना की है; सपा ब्लॉक श्रृंखला में पिओपि प्रकाशनों की समयबद्धता अपने वजन निर्धारित करते हैं, और एक विशेष ऊंचाई पर एक एसआई ब्लॉक श्रृंखला ब्लॉक के एक पिओपि प्रकाशन की समयबद्धता किसी भी माना जाता है की किसी भी S। ब्लॉक चेन ब्लॉक के पहले प्रकाशन के सापेक्ष है फोर्क्स ।

5.1 SP ब्लॉक श्रृंखला ट्रैकिंग

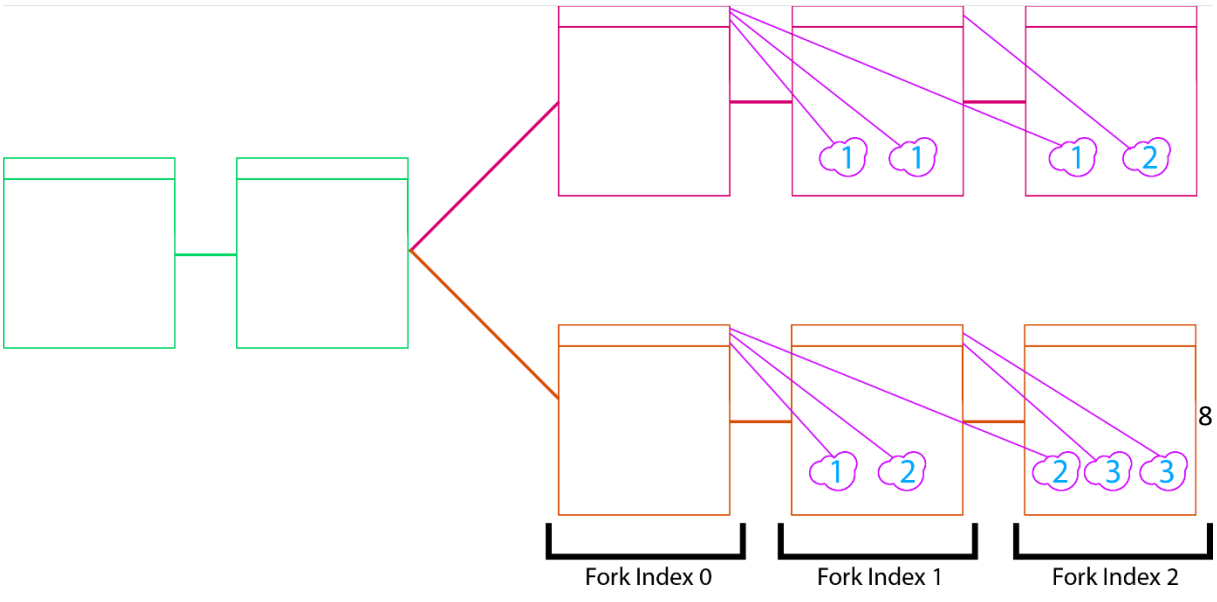
आदेश में S। ब्लॉक चेन नेटवर्क पर एक सहकर्मी के लिए संकल्प दोराहे करने के लिए, सहकर्मी का निर्माण और सपा ब्लॉक श्रृंखला के सभी S। ब्लॉक श्रृंखला ब्लॉकों के सभी द्वारा प्रदान की सभी का उपयोग कर के एक संस्करण का मूल्यांकन करना चाहिए (उन सहित हर संभावित दोराहे पर आर जो ग्राहक ज्ञान है) । आदेश में ऐसा करने के लिए, सहकर्मी S। ब्लॉक चेन ब्लॉक से हर एक सपा ब्लॉक चेन हैडर इकट्ठा, और सपा ब्लॉक श्रृंखला के नियमों के अनुसार आम सहमति निर्धारित करता है ("भारी" या श्रृंखला बनाने के लिए सबसे अधिक गणनाशक्तिकीआवश्यकताकोखोजने)।

सभी संभावित फोर्क जब सपा ब्लॉक श्रृंखला के पुनर्निर्माण से उपलब्ध जानकारी का उपयोग करके, सहकर्मी सुनिश्चित कर सकते है कि जो कुछ भी अंतिम तस्वीर वे सपा ब्लॉक श्रृंखला के मिल नवीनतम समय पर सपा ब्लॉक श्रृंखला के राज्य का प्रतिनिधित्व करता है ब्लॉक के किसी भी और टी में से किसी में वह फोर्क बनाया, मूल्यांकन के लिए अनुमति लगभग के रूप में अगर सहकर्मी सपा ब्लॉक श्रृंखला की पूरी तरह से सीधी पहुंच गया था ।
इस प्रणाली के माध्यम से, किसी भी दो विशेष श्रृंखला के सापेक्ष वजन पर गणना की जा सकती है साथियों जो समय में एक बाद में बिंदु पर नेटवर्क में शामिल होने से मांग । इस प्रणाली के माध्यम से, किसी भी दो विशेष श्रृंखला के सापेक्ष वजन पर गणना की जा सकती है साथियों जो समय में एक बाद में बिंदु पर नेटवर्क में शामिल होने से मांग ।

5.2 फोर्क वजन गणना

दो होड़ फोर्क का वजन सभी ब्लॉक के लिए जो दो चेन हट जाना सभी के स्कोर के सभी संक्षेप द्वारा गणना की है । कई फोर्क के बीच प्रतिस्पर्धा ब्लॉकों के स्कोर एक दूसरे के सापेक्ष गणना कर रहे हैं, एल्गोरिथ्म के बाद:

- ऊंचाई n पर सभी प्रतिस्पर्धी ब्लॉकों के लिए, प्रत्येक श्रृंखला है कि मैच में सभी PoP खनन लेनदेन मिल ऊंचाई पर है चेन ब्लॉक कहा
  - सभी PoP खनन लेनदेन के लिए सभी प्रतिस्पर्धा जंजीरों से ऊंचाई n पर किसी भी ब्लॉक की पुष्टि, जल्दी से प्रकाशन के साथ एक मिल (ब्लॉक ऊंचाई से) सपा ब्लॉक श्रृंखला में । इस ऊंचाई को m के रूप में संग्रहीत करना
  - प्रत्येक प्रतिस्पर्धा ब्लॉक n के लिए :
    - प्रत्येक PoP खनन लेनदेन की पुष्टि के लिए ब्लॉक n :
      - PoP खनन लेनदेन सबसे लंबे समय तक ज्ञात में एक ब्लॉक करने के लिए प्रकाशित करता है, तो सपा ब्लॉक चेन कांटा:
        - m से SP ब्लॉकचैन प्रकाशन ऊंचाई में अंतर निर्धारित करें, मान तल जोड़ें (1/(अंतर + 1) * (अंतर + 1))) वर्तमान ब्लॉक n के लिए स्कोर करने के लिए



ऊपर चित्र में, एसआई ब्लॉकचैन दो प्रतिस्पर्धी जंजीरों (लाल और नारंगी) के साथ एक दोराहे, मुठभेड़ों । पॉप खनन लेनदेन के अंदर नीले रंग की संख्या सपा ब्लॉकचैन जो वे डेटा प्रकाशित की अनुक्रमणिका का प्रतिनिधित्व करते हैं । जटिलता के लिए नहीं दिखाया गया है सपा ब्लॉकचैन ब्लॉक दो कांटों में एंबेडेड है, जो सपा ब्लॉकचैन के पुनर्निर्माण और पॉप लेनदेन के बाद आदेश देने की अनुमति.

जो ब्लॉकचैन को स्वीकार करने के लिए निर्धारित करने के लिए, प्रत्येक सूचकांक में प्रत्येक ब्लॉक के लिए स्कोर एक ही सूची में अंय ब्लॉक के सापेक्ष गणना की है, और प्रत्येक श्रृंखला पर सभी ब्लॉकों के लिए स्कोर एक साथ जोड़ रहे हैं: पहले या तो कांटा में प्रतिस्पर्धा ब्लॉक के लिए PoP प्रकाशन 0 सूचकांक सचित्र सपा के सूचकांक 1 में था ब्लॉकचैन. दोराहे पर लाल ब्लॉक 0, R0, तीन पॉप प्रकाशनों जो सपा ब्लॉकचैन के सूचकांक 1 में होते है द्वारा समर्थन किया है, तो अपने स्कोर 3 * (1/((1 1 + 1) * (1-1 + 1))) = ३००; R0 = ३००. कांटा 0, O0, पर नारंगी ब्लॉक दो पॉप प्रकाशनों जो sp ब्लॉकचैन के सूचकांक 1 में होते है द्वारा समर्थन किया है, और एक पॉप प्रकाशन 2 सूचकांक में सपा ब्लॉकचैन में, इसलिए इसका स्कोर 2 * (1/((1-1 + 1) * (1-1 + 1))) + 1 * (1/((2-1 + 1) * (2-1 + 1))) = २२५; O0 = २२५. इसी प्रकार, R1 = 1 * (1/((2-2 + 1) * (2-2 + 1))) = १०० और O1 = 2 * (1/((3-2 + 1) * (3-2 + 1))) = ५०. किसी भी श्रृंखला में पिछले ब्लॉक किसी भी सबूत वजन कभी नहीं है, क्योंकि कोई ब्लॉक के बाद यह इसके लिए पॉप विज्ञापन शामिल करने के लिए आ गया है; R2 = 0 और O2 = 0 । संक्षेप में इन अप, लाल श्रृंखला का वजन है ३०० + १०० = ४००, और नारंगी श्रृंखला का वजन २२५ + ५० = २७५ है । ४०० > २७५ के बाद से, लाल श्रृंखला अधिक समर्थन ब्लॉकचैन है ।

4 POP खनन लेनदेन के लाल श्रृंखला शामिल किए जाने की तुलना में 5 POP खनन लेनदेन की नारंगी श्रृंखला के शामिल होने के बावजूद, लाल श्रृंखला लेनदेन के सापेक्ष समयबद्धता यह एक उच्च सबूत वजन है, यह बेहतर श्रृंखला बना रही है ।

5.3 फोर्क संकल्प डिजाइन औचित्य

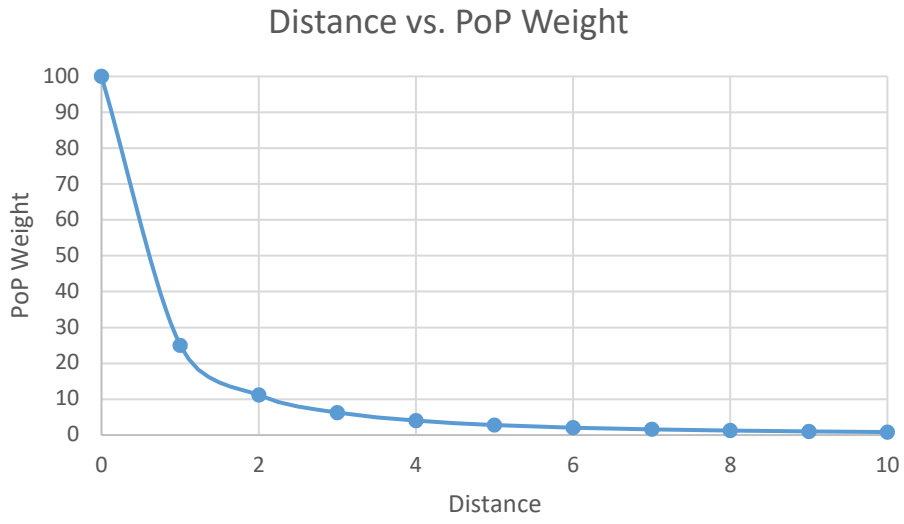
सपा ब्लॉकचैन में उनकी समयबद्धता के आधार पर POP खनन लेनदेन के सापेक्ष भार के उपयोग के लिए यह अविश्वसनीय रूप से मुश्किल एक हमलावर के लिए भविष्य में समय की किसी भी महत्वपूर्ण अवधि के दोराहे सपा ब्लॉकचैन ही बिना उत्पादन के लिए बनाता है.

जैसे, एक हमलावर वैध नेटवर्क के साथ ब्लॉकचैन के अपने संभावित दोराहे उत्पन्न करने की जरूरत है, और सपा ब्लॉकचैन में उनके Cl- फोर्क श्रृंखला के ब्लॉक हैश प्रकाशित करके पूर्ण सार्वजनिक दृश्य में ऐसा करना चाहिए । कोई भी फोर्क का निर्माण किया जा रहा है और लेनदेन को स्वीकार करने में देरी के लिए सपा ब्लॉकचैन निगरानी कर सकते है जब तक कांटा हल है, और Sl ब्लॉकचैन नेटवर्क अतिरिक्त सुविधाओं को लागू करने के लिए इन शेष के रूप में तंत्र का उपयोग जंजीरों को अमान्य कर सकते हैं यह नेटवर्क पर जारी किया गया है इससे पहले कि हमलावर श्रृंखला अमान्य है ।

5.4 भार समारोह

एक POP खनन लेनदेन के लिए सुझाव दिया भार समारोह मंजिल (1/(दूरी + 1) ^ 2) है, जहां दूरी अफोर्ड है POP खनन लेनदेन इसी SP ब्लॉक चेन ब्लॉक और पहली SP ब्लॉक श्रृंखला ब्लॉक के बीच दूरी वर्णित है जिसमें किसी भी एक ही सूचकांक में किसी भी माना जाता प्रतिस्पर्धी श्रृंखला के ब्लॉक सबसे पहले सपा ब्लॉक श्रृंखला के लिए प्रकाशित किया गया था । यह फार्मूला बेहतर एक विशेष Sl ब्लॉक श्रृंखला नेटवर्क की वांछित सुरक्षा प्रोफ़ाइल फिट करने के लिए फेरबदल किया जा सकता है । एक समारोह का उपयोग कर जो 0 तेजी के प्रति रुझान एक मौजूदा ब्लॉक श्रृंखला में परिणाम होगा

हमला करने के लिए आसान होने के नाते, लेकिन यह भी अल्पकालिक में कदम हमलों की संभावना बढ़ जाती है, जहां एक हमलावर उनके CI के एक ब्लॉक-हमला श्रृंखला एक SP ब्लॉक चेन ब्लॉक में इसी वैध SI चेन ब्लॉक से पहले नेटवर्क पर होता है पाने के लिए प्रयास करता है . यह सुझाव समारोह के रूप में हम अलग हमला परिदृश्यों के अधिक सिमुलेशन चलाने के लिए फेरबदल होना जारी रहेगा । निम्नलिखित ग्राफ का सुझाव दिया दूरी-बनाम-POP-भार फंक्शन को दर्शाता है ।



प्रत्येक बार फ़ंक्शन की गणना करने के बजाय, एक साधारण लुकअप तालिका का उपयोग किया जा सकता है:

Distance	Weight
0	100
1	25
2	11
3	6
4	4
5	2
6	2
7	1
8	1
9	1
>=10	0

किसी भी POP खनन लेनदेन संबंधित SI ब्लॉक चेन ब्लॉक सूचकांक के पहले प्रकाशन के बाद एक SP ब्लॉक चेन ब्लॉक 10 या अधिक SP ब्लॉक श्रृंखला ब्लॉक करने के लिए संगत कोई वजन नहीं है ।
के रूप में एक संभावित भेद्यता के समाधान के रूप में नीचे उल्लेख किया, एक समान भार योजना भी ब्लॉक के सापेक्ष स्कोर बिंदु के करीब प्राथमिकता लागू किया जा सकता है, यह सुनिश्चित करने के लिए कि SI ब्लॉक चेन फोर्क SP ब्लॉक श्रृंखला जल्दी करने की घोषणा की जरूरत है ।

6 संभावित हमले वैक्टर और शमन

सभी आम सहमति तंत्र के साथ के रूप में, एक विरोधी पार्टी को नेटवर्क पर सहमति स्थापित करने के लिए मजबूर करने का प्रयास कर सकते हैं । एक ठीक से लागू POP नेटवर्क पर, इन हमलों वैक्टर SP ब्लॉक श्रृंखला फोर्क और निर्माण और एक वैकल्पिक SI ब्लॉक श्रृंखला साबित शामिल हैं । POP के डिजाइन निर्णय के कुछ सरल सैद्धांतिक POP के अंय संभावित हमले वैक्टर को खत्म करने की तरह कार्यान्वयन।

6.1 CP ब्लॉक चेन फोर्क

घटना में है कि एक विरोधी पार्टी सफलतापूर्वक SP ब्लॉक श्रृंखला कांटे, वे फिर से नए POP डेटा के साथ कांटे SP ब्लॉक श्रृंखला ब्लॉकों लिख सकते हैं, उन्हें एक उच्च POP वजन के साथ एक SI ब्लॉक श्रृंखला का उत्पादन करने के लिए सक्षम करने से. राशि/लंबाई (वास्तविक दुनिया समय में मापा, ब्लॉक नहीं) SI ब्लॉक श्रृंखला वे फिर से लिखना करने में सक्षम है लगभग दूरी वे सफलतापूर्वक SP ब्लॉक श्रृंखला के लिए फोर्क के बराबर है.

नोट करें कि एक SI ब्लॉक श्रृंखला फोर्क करने के लिए विशिष्ट इरादे के बिना SP ब्लॉक श्रृंखला के एक फोर्क नहीं परिणाम होगा । हालांकि, SP ब्लॉक श्रृंखला के इस तरह के एक पुनर्गठन SI ब्लॉक चेन POP खनन लेनदेन जो कांटे की SP ब्लॉक श्रृंखला ब्लॉकों में हुई अब SP ब्लॉक श्रृंखला में मौजूद कारण होगा, और इस तरह कोई वजन पकड़ो । आगे अनुसंधान के एक क्षेत्र है कि क्या, अगर हमलावर अभी भी अपने नए ब्लॉकों में POP प्रकाशनों शामिल अपने लेनदेन की फीस कमाने के लिए, प्रक्रिया के कुछ प्रकार के POP खनिकों द्वारा इस्तेमाल किया जा सकता है फिर से नए SP ब्लॉक श्रृंखला पर अपने पुराने 'सबूत उपस्थिति प्रदर्शन ।
घटना में है कि SP ब्लॉक चेन कांटे पर ऐसा नहीं करता है, लेकिन SI ब्लॉक चेन पर हमला करने के लिए, और si ब्लॉक चेन के POP खनन लेनदेन प्रभावित कर रहे हैं और अब वजन पकड़, SI ब्लॉक चेन की वर्तमान सुरक्षा अपने स्वयं के मध्यवर्ती करने के लिए नीचे छोड़ देंगे (POW/ POS/आदि) आम सहमति तंत्र जब तक POP खनिक सपा ब्लॉक श्रृंखला के लिए नए ब्लॉकचैन राज्य डेटा प्रकाशित और POP खनन लेनदेन वापस SI ब्लॉक श्रृंखला के लिए प्रदान करते हैं ।

6.2 एक वैकल्पिक उच्च प्रूफ वजन SI ब्लॉक चेन निर्माण

इस हमले के प्रदर्शन की आवश्यकता है कि विरोधी पार्टी एक वैकल्पिक SI श्रृंखला है जो वर्तमान सबसे अच्छा SI श्रृंखला की तुलना में एक उच्च सबूत वजन है का निर्माण । आदेश में इस हमले को सफलतापूर्वक निष्पादित करने के लिए (सबूतों के कारण उनकी समयबद्धता पर मूल्यांकन किया जा रहा है), एक हमलावर अपने हमला ब्लॉक श्रृंखला के साथ साथ (या तेजी से) वर्तमान SI श्रृंखला का निर्माण करने की आवश्यकता होगी. यह हमलावर उनके आक्रमण श्रृंखला के ब्लॉक चेन स्थिति डेटा SP ब्लॉक चेन तुरंत प्रकाशित करें, नेटवर्क के उपयोगकर्ताओं को लंबित हमले और उसके गुण देखने के लिए अनुमति देने की आवश्यकता है । जैसे, SP ब्लॉक श्रृंखला देख किसी को क्या ब्लॉक को कांटा, कितना मजबूत (या कमजोर) वर्तमान श्रृंखला के लिए जोखिम में है देखना होगा विरोधी पार्टी की श्रृंखला की तुलना में है, और संभवतः कुछ का उपयोग कर सकता है (जैसे संतुलन आधारित मतदान) को अमान्य विरोधी श्रृंखला से पहले यह नेटवर्क के लिए जारी की है ।

एक और संभव में (हालांकि अधिक कठिन) कार्यांवयन, हमलावर एक वैकल्पिक SI श्रृंखला जिसका पहले ब्लॉकों में छोटे-से-कोई सबूत वजन जब वर्तमान श्रृंखला की तुलना में निर्माण होता है, लेकिन जिसका बाद में ब्लॉक बड़े पैमाने पर सपा के लिए प्रकाशित कर रहे है ब्लॉकचैन. हमले के इस तरह अभी भी सार्वजनिक रूप से सपा ब्लॉकचैन पर प्रकाशनों के कारण दिखाई है, लेकिन यह जरूरी नहीं कि कितनी दूर वापस फोर्क हो सकता है प्रकट होगा, और भी समय पर नेटवर्क के उपयोगकर्ताओं को नहीं दिखाई देगा जब आक्रमण के पहले ब्लॉकों में से कुछ किंग चेन बिना प्रूफ वजन के बनवाए जा रहे थे. इस हमले को कम करने के लिए, ब्लॉक श्रृंखला नेटवर्क बस वजन काफी अधिक वजन के साथ बिंदु दोराहे के करीब ब्लॉकों (इतनी राशि १०० * weight0 + ७० * weight1 + ५५ * weight2 की तरह कुछ लग सकता है...), इस हमले मुश्किल या असंभव को सफलतापूर्वक बनाने प्रदर्शन.

6.3 फर्जी SI ब्लॉक चेन स्टेट डाटा का प्रकाशन

एक POP कार्यान्वयन के एक संस्करण में जहां SI ब्लॉक श्रृंखला राज्य डेटा SP ब्लॉक श्रृंखला के लिए प्रकाशित डेटा की संभावित वैधता की पुष्टि करने के लिए पर्याप्त नहीं है, एक विरोधी पार्टी जाली बनाना द्वारा लेनदेन को स्वीकार करने में देरी करने के लिए नेटवर्क पर पार्टियों का कारण बन सकता है एक संभावित कांटा जो वास्तव में मौजूद नहीं है । इस हमले मध्यवर्ती आम सहमति की आवश्यकता नहीं है, लेकिन केवल हमलावर एक उपद्रव होने की अनुमति देता है क्योंकि नेटवर्क अगर हमलावर पूरा ब्लॉकों के लिए जो डेटा SP ब्लॉक श्रृंखला के लिए टैग मौजूद है प्रदान नहीं कर सकता फोर्क नहीं होगा । इस हमले हमलावर जाहिरा तौर पर वैध ब्लॉक श्रृंखला राज्य डेटा जिसके लिए वे वास्तव में ब्लॉक के लिए नहीं है प्रकाशन शामिल है ।

एक SI ब्लॉक श्रृंखला जो तुरंत आम सहमति के लिए POW पर निर्भर करता है, यह आवश्यकता द्वारा कम किया जा सकता है, POP के रूप में वर्तमान में है, पूरे ब्लॉक हेडर के प्रकाशन । इस तरह, हमलावर फर्जी SI ब्लॉक चेन डेटा प्रकाशित नहीं कर सकता क्योंकि डेटा एक मान्य POW समाधान नहीं होगा ।

एक SI ब्लॉक चेन में POS रोजगार, यह भी अतिरिक्त सिक्का आयु या इसी तरह के नेटवर्क संपत्ति-आधारित खनन संसाधनों, या जो पूर्ण नोड्स के रूप में सूचित नेटवर्क प्रतिभागियों द्वारा सत्यापित किया जा सकता है की स्वामित्व साबित जानकारी प्रकाशित करने के लिए संभव है (txid युक्त का दावा करने के लिए खर्च, आदि) सिक्का ।

7 POS के साथ संयोजन

पॉप ब्लॉक (या आम सहमति के अंय असतत इकाइयों) बनाने और अल्पकालिक बनाए रखने के एक मध्यवर्ती विधि की आवश्यकता है अवधि के लंबित सहमति पॉप प्रकाशनों । एक मध्यवर्ती आम सहमति तंत्र के रूप में पाउ का उपयोग कर नेटवर्क पर पॉप को लागू करने सीधे आगे है, है पॉप पाउ के प्राकृतिक विस्तार की तरह आम सहमति दी । एक पॉस नेटवर्क पर PoP को कार्यान्वित अतिरिक्त विचार की आवश्यकता है, और शुद्ध पॉस के साथ लंबी-खड़ी समस्याओं के लिए समाधान प्रदान करता है ।

7.1 मौजूदा पॉस समस्याएँ

नोट: POS के कई उपकरणों मौजूद है । स्थिति एक आम सहमति एल्गोरिथ्म नहीं है, बल्कि कई बारीकी से संबंधित आम सहमति एल्गोरिदम का एक संग्रह है जो साझा विशेषता

"शेष-आधारित" (या खर्च-निर्गम-आधारित) खनन, जिसमें खनिक ब्लॉकों का उत्पादन करने के लिए अपने मूल टोकन संतुलन का उपयोग करते हैं, और खनन का "संसाधन व्यय" टोकन का समय-मूल्य होता है । POS के मूल पीरकॉइन कार्यांवयन में मौजूद कुछ मुद्दे (जैसे कि लंबी दूरी की नियत हिस्सेदारी संशोधक के कारण हमलों) नए PoS कार्यान्वयन द्वारा हल किया गया है, और उन मुद्दों को हल यहां चर्चा के लिए पुनर्जीवित नहीं किया जाएगा ।

दो प्राथमिक मुद्दे POS के नवीनतम पुनरावृत्ति का सामना:

1. वहां कोई तरीका नहीं गणितीय बूटस्ट्रैपिंग के दौरान एक नया नोड के लिए एक ब्लॉकचैन की वैधता का प्रदर्शन है (श्रृंखला है "कमजोर मनोवाद") ।
2. वहां केवल एक अल्पकालिक समाधान है (पिछले ' n ' ब्लाकों) "दांव पर कुछ भी नहीं" समस्या है ।

इन दोनों मुद्दों के मनोवाद के लिए फ़ॉलबैक-निजी एक ब्लॉकचैन के इतिहास में एक मनमाना बिंदु पर नेटवर्क टोकन स्वामित्व के एक ' महत्वपूर्ण जन ' का प्रतिनिधित्व कुंजी के एक नंबर के लिए नेटवर्क सप्ताह, महीने, या वर्ष का एक और वैध कांटा उत्पादन किया जा सकता है अतीत में, और किसी भी टोकन के वर्तमान स्वामित्व की आवश्यकता नहीं है । इसके अतिरिक्त, यह साबित करना असंभव है कि कोई पार्टी नेटवर्क टोकन के एक महत्वपूर्ण जन तक पहुंच है । स्लैश प्रोटोकॉल एक दंडात्मक प्रणाली को हल "दांव पर कुछ नहीं" अल्पकालिक में समस्याओं को प्रस्तुत करता है.

7.2 बूटस्ट्रैपिंग के दौरान वैधता का गणितीय प्रदर्शन

पारंपरिक PoW सिस्टम के एक उद्देश्य परिभाषा "सबसे अच्छा ब्लॉकचैन," (ब्लॉकचैन जो निर्माण करने के लिए सबसे संचयी कार्य की आवश्यकता है) और यह मानते हुए कि एक बूटस्ट्रैपिंग नोड ब्लॉकचैन नेटवर्क के लिए अप्रतिबंधित पहुँच है, नोड हमेशा सक्षम हो जाएगा को स्वतंत्र रूप से श्रेष्ठ ब्लॉकचैन का निर्धारण करना. शुद्ध-PoS प्रणालियों में, एक सामने बताया महत्वपूर्ण जन स्वामित्व समस्या के समाधान के लिए बस है, प्रोटोकॉल के भाग के रूप में, ब्लॉक के एक निश्चित संख्या से अधिक वापस कांटे से किसी भी नोड को रोकने के । एक रोलिंग जांच प्रणाली में इस तरह के एक प्रणाली परिणाम जिसमें प्रत्येक नोड बस ब्लॉक ' n ' की एक निश्चित संख्या से अधिक हटाने के लिए अपने वर्तमान ' सर्वश्रेष्ठ ' ब्लॉकचैन दृश्य से मना कर दिया । जैसे, अगर एक ग्राहक पुराने सिक्का स्वामित्व का उपयोग करता है एक कांटा जो n ब्लॉक पहले से अधिक शुरू होता है बनाने के लिए, नेटवर्क पर नोड्स बस कांटा अस्वीकार करेगा. हालांकि, एक बूटस्ट्रैपिंग ग्राहक नाजायज ब्लॉक श्रृंखला पहले खिलाया जा सकता है, और बाद में वापस से अधिक n ब्लॉक नाजायज श्रृंखला पर वापस फोर्क मना, स्थाई रूप से (मानवीय हस्तक्षेप के बिना) उंहें सही ब्लॉक श्रृंखला पर नज़र रखने से रोकने । POP इस समस्या के लिए एक सरल समाधान प्रदान करता है, एक ब्लॉक श्रृंखला POP का उपयोग कर के रूप में एक गणितीय निरीक्षण "सबसे अच्छा ब्लॉक श्रृंखला" एक POW SP ब्लॉक श्रृंखला में ब्लॉक श्रृंखला शामिल किए जाने से परिभाषित किया जाएगा ।

7.3 n ब्लॉक से अधिक "स्टेक पर कुछ नहीं समाधान"

लंबे समय में "दांव पर कुछ नहीं" समाधान के वर्तमान समाधान के लिए ग्राहकों को कांटों की अनदेखी है कि वर्तमान ब्लॉकचैन से अधिक एक्स ब्लॉकों को हटाने के लिए है, के रूप में ऊपर समझाया ।

करने के लिए मना कर एक ब्लॉकचैन पुनर्गठन से अधिक n ब्लॉक गहरी एक दिलचस्प हमले वेक्टर प्रस्तुत करता है: एक ब्लॉकचैन पर फोर्क जो एक नया ब्लॉक के प्रचार के दौरान बिल्कुल y इतिहास के ब्लाकों फोर्क की तैनाती, नेटवर्क के भाग जा (जो अभी तक नवीनतम ब्लॉक नहीं देखा है और जैसे वापस एक्स ब्लॉक फोर्क करने को तैयार) स्थाई रूप से (मानव हस्तक्षेप के बिना) नेटवर्क है जो पहले से ही नए ब्लॉक प्राप्त किया था के भागों से सिंक्रनाइज़ वापस एक्स 1 ब्लॉकों फोर्क मना कर दिया । इस हमले के दिखावट और संभावित नुकसान बढ़ ब्लॉक प्रसार के समय के साथ बढ़ता है, जो बड़ा और अधिक से परिणाम कर सकते है-जटिल-को मांय ब्लॉकों । चूंकि हम कहीं भी इस प्रकार के हमले का कोई उल्लेख नहीं पा रहे थे, हम इसे परिशिष्ट A में वर्णित करते हैं ।

POP लागू करने से यह सुनिश्चित होता है कि एक ब्लॉक श्रृंखला के इतिहास में एक निश्चित समय पर सिक्कों के स्वामित्व के एक महत्वपूर्ण जन के अधिग्रहण के लिए नेटवर्क पर हमला नहीं किया जा सकता है, क्योंकि साथ POP प्रकाशनों या तो गैर विद्यमान या अप्रासंगिक होने के कारण होगा अनहोनी, ग्राहकों को अधिकतम फोर्क दूरी के बारे में नियम को दूर करने की अनुमति, ब्लॉक श्रृंखला के किसी भी महत्वपूर्ण हिस्से फोर्क के बाद से सफलतापूर्वक और एक साथ SP ब्लॉक श्रृंखला पर हमला करने की आवश्यकता होगी ।

वास्तव में, सफल गैर एक ब्लॉक अधिनियम के एक प्रभावी "नरम अधिकतम दूरी कांटा," के रूप में मजबूत बढ़ के रूप में एक निश्चित बिंदु से पहले से एक कांटा बनाने की कठिनाई के रूप में तैयार पॉप विज्ञापन लड़ा के रूप में विकसित हो जाता है बेहद अकल्पनीय पॉप भार के कारण एल्गोरिदम.

8 परिशिष्ट A: सीमित रीऑर्ग दूरी भंग करना आक्रमण

8.1 POS में अल्पकालिक आम सहमति की सुरक्षा की समीक्षा

अल्पावधि में, शुद्ध-POS ब्लॉक चेन "दांव पर कुछ नहीं" से बचने के लिए एक निश्चित अवधि के लिए जमा (या आस्तियों के ठंड) की आवश्यकता से बच सकते है क्रम में उन सिक्कों पर PoS खनन सक्षम करने के लिए (एक विधि इथेरियम के लिए विचार किया, और इथेरियम द्वारा ' स्लैश ' शब्द डेवलपर्स). सामान्य POS सिस्टम में, सभी संभव कांटे के शीर्ष पर POS ब्लॉक का उत्पादन करने के प्रयास में एक नगण्य लागत है । जब एक स्थिति खान में काम करनेवाला दो या अधिक प्रतिस्पर्धी ब्लॉक प्राप्त करता है, यह अपने सर्वोत्तम हित में है दोनों चेन, या संभावित प्रतिस्पर्धा ब्लॉकों जो वे ऊपर मेरा करने में असमर्थ है के किसी भी रोक पर बनाने का प्रयास । हालांकि, ठंड संपत्ति के द्वारा, नेटवर्क खनिक जो "इनाम शिकारी" इस प्रकार के व्यवहार के लिए देखने के लिए अनुमति देकर इस व्यवहार का अभ्यास सज़ा कर सकते हैं, क्रिप्टोग्राफिक सबूत प्रदान (जैसे ही खान में काम करनेवाला है जो एक ही में प्रतिस्पर्धा ब्लॉकों के लिए वोट से दो हस्ताक्षर ऊंचाई), और जमे हुए सिक्कों का एक हिस्सा प्राप्त करते हैं ।

भोली अल्पकालिक कांटा हमलों कुल नेटवर्क जताया सिक्कों का एक महत्वपूर्ण भाग के तुरंत हमले से पहले स्वामित्व की आवश्यकता है, उंहें मोटे तौर पर अकल्पनीय और लाभकर बना ।
ब्लाक कॉइन और न्यूकॉइन जैसी परियोजनाओं द्वारा कार्यांवित किए गए और गतिशील हिस्सेदारी संशोधक से पहले कम सिक्का उंर के कारण अल्पावधि में "हिस्सेदारी पीस" हमला भी अप्रभावी है । इन मुद्दों को पाउ नेटवर्क में मौजूद नहीं है, के रूप में अभिकलनी एक श्रृंखला पर बनाने का प्रयास खर्च किया जा सकता है एक और श्रृंखला पर बनाने का प्रयास खर्च नहीं है ।

8.2 लंबी अवधि के आक्रमण

लंबी अवधि में आम सहमति की रक्षा के अधिकांश साधन अप्रभावी हैं । जमे हुए जमा अंततः वापस आ रहे हैं, समय की लंबी अवधि हमलावरों सिक्के में अपनी पूरी स्थिति को बेचने के लिए या निजी चाबी है जो जताया सिक्कों का एक बड़ा हिस्सा बहुत पहले आयोजित प्राप्त करने की अनुमति, और हमलों के बाद से संभव हो पीस एक हमलावर करने में सक्षम मज़बूती से अतीत में अब तक ब्लॉक श्रृंखला के एक महत्वपूर्ण जन को फिर से लिखना संभव ब्लॉक श्रृंखला की एक संख्या का पता लगाने कर सकते हैं (प्रत्येक अलग लेनदेन के आदेश के साथ, जो दांव संशोधक की तरह बातें बदल) केवल उनके उपलब्ध अभिकलनी शक्ति से बंधे. यह टोकन स्वामित्व/दूर ब्लॉक श्रृंखला के अतीत में, पर्याप्त अभिकलनी शक्ति दी, वर्तमान ब्लॉक श्रृंखला से एक अधिक वैध ब्लॉक श्रृंखला बनाने के एक महत्वपूर्ण जन की अनुमति देता है ।
एक हमलावर के इस फार्म का संचालन करने का प्रयास जरूरी टोकन के किसी भी वर्तमान में ही नहीं है, और अधिक होने की संभावना है सेवाओं में एक बड़े पैमाने पर व्यवधान के कारण डबल प्रदर्शन में से खर्च करता है.

8.3 वर्तमान लंबी अवधि के आक्रमण समाधान

आदेश में ब्लॉकचैन इतिहास के संभावित वर्षों के लेखन से लंबी अवधि के हमलों की संभावना को खत्म करने के लिए, ग्राहकों को स्थिति नेटवर्क पर बस को स्वीकार नहीं क्रमादेशित रहे है

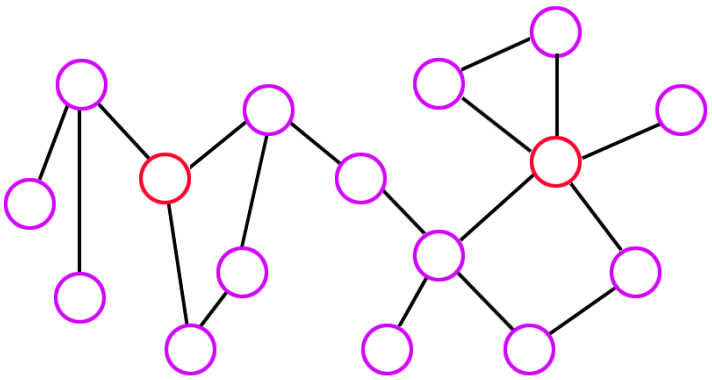
पुनर्गठन जो नेटवर्क ' n ' ब्लॉक पहले से अधिक कांटा । यह संभव नए बूटस्ट्रैपिंग साथियों के लिए स्थाई रूप से एक गलत दोराहे पर फंसे होने के लिए बनाता है, लेकिन सामांय ऑपरेशन के तहत जो हमेशा जुड़े रहे है नोड्स के लिए किसी भी संभावित व्यवधान पैदा नहीं करता है, या अधिक बार से कनेक्ट करने के लिए n ब्लॉक जोड़ने के नेटवर्क लेता है ।

मान n को अधिकतम पुनर्गठन गहराई के रूप में चुना कई कारकों पर निर्भर करता है, जिसमें अवधि के लिए जो सिक्के अवरोधित है (यदि एक जमा-आधारित POS सिस्टम पर, के रूप में स्लैश का प्रस्ताव), एक हमलावर के लिए अपेक्षित समय पुराने निजी कुंजी प्राप्त करने के लिए/ मुद्रा में स्थिति, नेटवर्क पर ब्लॉक की गति, आदि एक n के बहुत छोटे यह संभव नेटवर्क के लिए आसानी से सिंक्रनाइज़ करने के लिए बनाता है (के बाद भी बेहद मुश्किल हमलों बहुत कम संभावना के कारण समय अवधि में प्रशंसनीय हैं), और एक n के बहुत बड़े लंबे समय तक हमलों अधिक प्रभावोत्पादक बनाता है ।

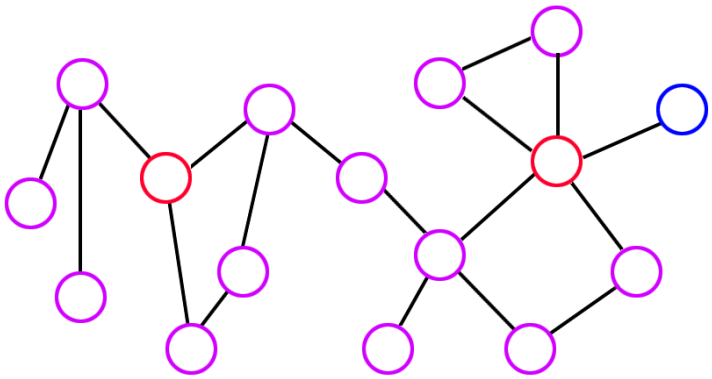
8.4 अधिकतम पुनर्गठन गहराई के साथ समस्याएं

घटना में है कि एक हमलावर एक कांटा है जो सही ब्लॉकचैन n ब्लॉक पहले से हट जाता बनाने में सक्षम था, हमलावर इस दोराहे जबकि वर्तमान ब्लॉक अभी भी नेटवर्क भर में प्रचार कर रहा है जारी सकता है (नेटवर्क पर कुछ साथियों अर्थ एक पर है दूसरों की तुलना में अलग ब्लॉक) ।

न्यूकॉइन की तरह एक ब्लॉकचैन पर जहां अधिकतम पुनर्गठन गहराई ४३,८३० ब्लॉकों है, अगर नेटवर्क पर मौजूदा ब्लॉक ऊंचाई १४३,८३० था, तो एक कांटा जो नेटवर्क वापस १००,००० ब्लॉक के कांटे जारी सभी साथियों द्वारा स्वीकार किया जाएगा । हालांकि, जारी १००,००० ब्लॉक वापस कांटा एक बार नेटवर्क १४३,८३१ ब्लॉक में है किसी भी परिणाम नहीं होगा ।

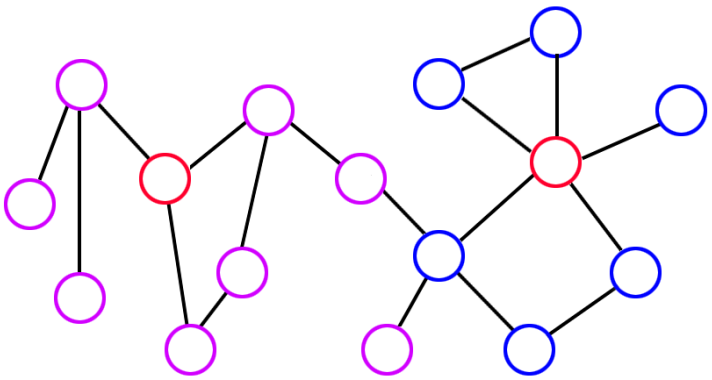


= Node on Block 143,830 = Attacker Node

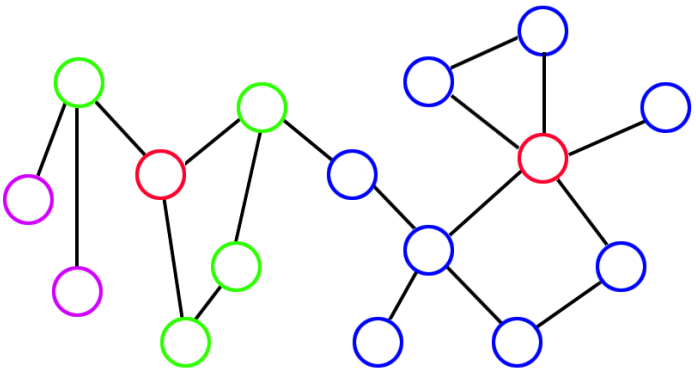


= Node on Block 143,831_a

Attacker learns of block 143,831 from one owned node

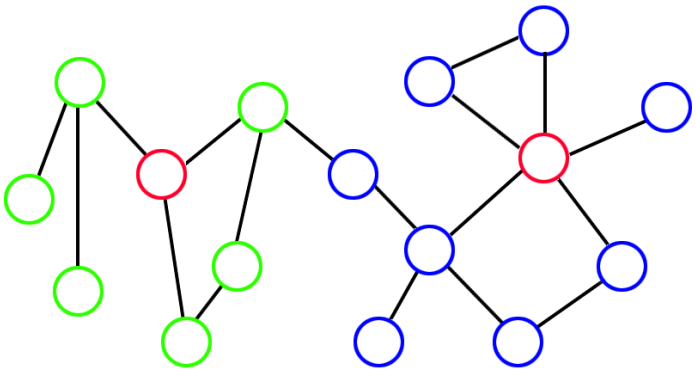


Propagation of Block 143,831_a continues



= Node on Block 143,831_b

Attacker releases fork back to 100,000 which ends with block 143,831_b



Network settles, nodes on block 143,831_a and block 143,831_b are unable to reach consensus because they diverge at block 100,000, and switching from _a to _b or from _b to _a would require a reorganization deeper than 43,830 blocks.

नेटवर्क के कारण/नए ब्लॉकों के प्रसंस्करण विलंबता, पूरे नेटवर्क के बीच एक अवधि है १४३,८३० ब्लॉक पर जा रहा है और पूरे नेटवर्क ब्लॉक १४३,८३१ पर जा रहा है । इस अवधि के दौरान, ध्यान से वितरित और अच्छी तरह से जुड़े नोड्स हमलावर द्वारा नियंत्रित अपने साथियों के लिए कांटा जारी सकता है जैसे ही ब्लॉक १४३,८३१ पहले नेटवर्क पर मनाया जाता है । जैसे, साथियों जो केवल १४३,८३० ब्लॉक के बारे में पता कर रहे है कांटा स्वीकार करेंगे और इतिहास के ४३,८३० ब्लॉकों अधिलेखित (और कांटा है, जो १४३,८३१ हो सकता है के अंतिम खंड पर समाप्त होगा) । हालांकि, साथियों जो वैध ब्लॉक १४३,८३१ पहले नेटवर्क भर में प्रचार दोराहे स्वीकार नहीं करते हैं । इस बिंदु पर, नेटवर्क दो खंडों, जो दोनों एक जाहिरा तौर पर वैध ब्लॉक १४३,८३१ है में खंडित है । विभाजन के दो पक्षों में सक्षम सामंजस्य और निर्धारित नहीं है जो ब्लॉकचैन सही है, या तो दूसरे पक्ष के ब्लॉकचैन स्वीकार एक पुनर्गठन ४३,८३१ ब्लॉक गहरी है, जो कोई ग्राहक मानव हस्तक्षेप के बिना प्रदर्शन करेंगे की आवश्यकता होगी, के रूप में प्रति प्रोटोकॉल ।

एक गैर दंडात्मक स्थिति प्रणाली में जहां इष्टतम स्वयं सेवारत खनन रणनीति सभी उपलब्ध ब्लॉक चेन कांटे पर खनन शामिल है, यह संभव है कि कई प्रतिस्पर्धी कांटे एक लंबे समय से पहले आम बिंदु से उपजी समानांतर में बनाया जा करने के लिए जारी है । जब इन प्रतिस्पर्धा कांटे के एक आम पूर्वज के बाद से लंबाई n तक पहुंचता है, ग्राहकों को स्थाई रूप से एक दूसरे से सिंक्रनाइज़ होने की संभावना के रूप में वे व्यक्तिगत रूप से इन कांटों में से एक का चयन और किसी अंय कांटा कांटा से मना करने के बाद से दूसरे कांटे संगठनों की आवश्यकता होती है जो गहरे हैं वे प्रदर्शन करने को तैयार हैं ।

8.5 **शमन**

इस हमले की आवश्यकता है कि n पर्याप्त बड़ी है कि एक हमलावर सफलतापूर्वक एक "स्व-बनाए रखने" ब्लॉक चेन निजी अतीत में स्वामित्व वाली कुंजियों पर आधारित है, या कि n पर्याप्त रूप से छोटा है कि एक दूरी n के छोटे अवधि के हमलों का निर्माण करने के लिए व्यावहारिक है बना सकते हैं । एक मान के लिए n सेटिंग जहां तक संभव हो दोनों चरम सीमाओं से इस आक्रमण को निष्पादित करने के लिए एक हमलावर की क्षमता को कम करता है ।

वैकल्पिक रूप से, POP को लागू करने के लिए एक अधिकतम पुनर्गठन गहराई की आवश्यकता को हटा (और यह लगभग असंभव बनाता है के लिए एक लंबे समय तक पुनर्गठन का उत्पादन किया जा), इस स्थाई डी तुल्यकालन हमले के लिए क्षमता को नष्ट करने ।

9 परिशिष्ट B: वेरीब्लॉक ब्लॉक चेन

अधिकांश ब्लॉक चेन बिटकॉइन से आम सहमति सुरक्षा का वारिस करना चाहते हैं । सीमित ब्लॉक आकार और बढ़ती लेनदेन फीस, 10 मिनट के ब्लॉक समय, ८०-बाइट सीमा से OP_RETURN के साथ प्रकाशित डेटा को कम करने के लिए, और असंगठित संयुक्त राष्ट्र से संबंधित डेटा की बड़ी मात्रा बिटकॉइन ब्लॉक श्रृंखला के माध्यम से सॉर्ट करने के लिए, हम प्रस्ताव एक मध्यस्थ एकत्रीकरण ब्लॉक श्रृंखला: वेरीब्लॉक. वेरीब्लॉक POP का उपयोग कर बिटकॉइन के साथ सीधे सुरक्षित करने के लिए बनाया गया है, और अन्य ब्लॉक श्रृंखला बिटकॉइन करने के लिए कुल में प्रॉक्सी द्वारा प्रकाशित हो जाता है जो वेरीब्लॉक, सीधे ब्लॉक श्रृंखला राज्य डेटा प्रकाशित करने के लिए अनुमति देते हैं ।

9.1 वेरीब्लॉक के साथ घालमेल

एक ब्लॉक श्रृंखला वेरीब्लॉक के साथ सुरक्षित वेरीब्लॉक और बिटकॉइन आम सहमति स्वचालित रूप से ट्रैक करने के लिए एक प्रदान की पुस्तकालय का उपयोग करें, और फिर अपने ब्लॉक स्वरूप और इनाम संरचना थोड़ा बदल जाएगा और समायोजित करने के लिए POP खनिकों को पुरस्कृत, और उनके नियमों का अद्यतन कांटों को हल करते समय वेरीब्लॉक लाइब्रेरी को क्वेरी करने के लिए नेटवर्क सहमति.

9.2 वेरीब्लॉक डिजाइन

वेरीब्लॉक एक POW-आधारित नेटवर्क पॉप के साथ बिटकॉइन के लिए सीधे सुरक्षित एक मिनी ब्लॉक श्रृंखला पर सरल लेनदेन (कोई पटकथा) को संभालने के लिए डिज़ाइन किया गया है । एक तेजी से ब्लॉक समय (जैसे 1 मिनट) प्रकाशन परिवर्तनशीलता कम कर देता है, डेटा की बड़ी मनमाना टुकड़े के लेनदेन समर्थन प्रकाशन (POS और dPoS नेटवर्क का उपयोग करने के लिए पर्याप्त), और वेरीब्लॉक POW खनिक स्वचालित रूप से कई सरल एकत्रीकरण का पालन करें प्रकाशित डेटा के सारांश प्रदान करने के लिए नियम (प्रकाशित डेटा के उपसर्ग के आधार पर POP लेन-देन का आदेश देते हैं, जो प्रत्येक नेटवर्क के लिए संभावित रूप से प्रासंगिक जानकारी को एक साथ समूहीकृत करता है). इसके अतिरिक्त, वेरीब्लॉक ब्याज की किसी भी एसआई ब्लॉक श्रृंखला पर जल्दी हमले सूचनाओं के लिए आसान सदस्यता प्रदान करने के लिए बनाया गया है । यह एक वातावरण प्रदान करता है, जहां एक व्यापारी, विनिमय, भुगतान प्रोसेसर, आदि एक जगह (वेरीब्लॉक) को ब्लॉक श्रृंखला वे में रुचि रखते है के सभी के बारे में सुरक्षा जानकारी प्राप्त है, तीसरे पक्ष के साथ सुरक्षित एकीकरण अविश्वसनीय रूप से सरल बना ।

9.3 वेरीब्लॉक लाभ

बिटकॉइन के लिए सीधे जाने के लिए, एक ब्लॉक श्रृंखला के लिए अपने ब्लॉक शीर्षक बदलने के लिए लगभग ६४ बाइट्स (बजाय सामान्य ८० के) POW नेटवर्क के लिए, या प्रकाशन के कहीं अधिक महंगा और मुश्किल मतलब का उपयोग करने के लिए चुनते हैं (जैसे "असंभव" पते की जरूरत है, में एकाधिक OP_RETURN एकाधिक लेनदेन, आदि) । इसके अतिरिक्त, ब्लॉक श्रृंखला को स्वयं बिटकॉइन के पूर्ण SPV-स्तरीय सर्वसंमति को बनाए रखने को लागू करने की आवश्यकता होगी, और इच्छुक उपयोगकर्ताओं को जल्दी हमले का पता लगाने के लिए पूरे बिटकॉइन ब्लॉक श्रृंखला को सुनने की आवश्यकता होगी ।

वेरीब्लॉक का उपयोग कर, वे अपने वर्तमान ब्लॉक स्वरूप रख सकते हैं, ब्लॉक श्रृंखला राज्य डेटा की बड़ी मात्रा में प्रकाशित करें (विशेष रूप से POS नेटवर्क जो हिस्सेदारी वजन के अस्तित्व को साबित करने के लिए संबंधित डेटा प्रकाशित करने की आवश्यकता के लिए उपयोगी एक pos खान में उपभोग करने के लिए भस्म करने का दावा है टकसाल एक ब्लॉक), प्रकाशनों और वजन के लिए एक तेजी से ब्लॉक समय का लाभ लेने के लिए उपयुक्त हमलों को दिखाई जल्दी हो व्यवहार्य हो, और एक उच्च स्तर है

उनके POP खनन के विकेंद्रीकरण की, क्योंकि प्रत्येक POP प्रकाशन कम लागत बिटकॉइन पर से वेरीब्लॉक पर प्रदर्शन करने के लिए ।

9.4 वेरीब्लॉक निर्भरता

एक ब्लॉकचैन जो सुरक्षा के लिए वेरीब्लॉक का उपयोग करने के लिए चुना वेरीब्लॉक नेटवर्क विफल रहता है जो इवेंट में कार्य करने के लिए बंद नहीं होगा । मौजूदा पॉप आम सहमति Sl ब्लॉक चेन खुद पर संग्रहीत है और अभी भी इस्तेमाल किया जा सकता है, और भविष्य आम सहमति बस वापस ब्लॉकचैन सामांय आम सहमति एल्गोरिथ्म के लिए गिर जाएगी (POW/POS/आदि) नए POP जानकारी के अभाव में ।

इसके अतिरिक्त, वेरीब्लॉक के प्रारंभिक हमले का पता लगाने के लाभों को छोड़ करने के लिए इच्छुक ब्लॉक चेन (या विकास प्रयास वेरीब्लॉक और बिटकॉइन एक साथ संभावित हमलों के लिए निगरानी में रखने के लिए तैयार) POP खनिकों वेरीब्लॉक उपयोग करने के लिए अनुमति दे सकते हैं या प्रदर्शन बिटकॉइन के लिए सीधे प्रकाशनों, वेरीब्लॉक समस्याओं की स्थिति में एक POP विफलता प्रदान करते हैं ।

References

[1] Peercoin Whitepaper [https://peercoin.net/assets/paper/peercoin-paper.pdf]

[2] BlackCoin PoS Whitepaper v2 [https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf]

[3] Neucoin Whitepaper [http://www.neucoin.org/en/whitepaper]

[4] Ethereum Blog Post on Weak Subjectivity [https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/]

[5] OmniLayer Specifications [https://github.com/OmniLayer/spec]

[6] Counterparty Specifications [http://counterparty.io/docs/protocol_specification/]

[7] Colored Coins Specifications [https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification]

[8] Merged Mining Specifications [https://en.bitcoin.it/wiki/Merged_mining_specification]

[9] ChainDB Whitepaper [https://bitpay.com/chaindb.pdf]