बिटकॉयनः इलेक्ट्रोनिक कैश का पियर-टू-पियर वर्ज़न

सातोशी नाकामोतो
www.bitcoin.org

सारः इलेक्ट्रोनिक कैश का शुद्ध रूप से पियर-टू-पियर वर्ज़न एक पार्टी से दूसरी पार्टी को सीधे ऑनलाईन भुगतान का आसान बनाएगा, जिसमें वित्तीय संस्थान की भूमिका नहीं होगी। डिजिटल सिग्नेचर आंशिक समाधान प्रदान करते हैं, लेकिन मुख्य लाभ नहीं मिल पाता, अगर भरोसेमंद थर्ड पार्टी के लिए दोहरा खर्च रोकना ज़रूरी हो। हमारा मानना है कि इस दोहरे खर्च का समाधान है पियर-टू-पियर नेटवर्क का उपयोग करना। नेटवर्क टाईमस्टैम्प लेनदेन को हैश कर, हैश-आधारित कार्य के प्रमाण में शामिल कर, ऐसा रिकॉर्ड बनाया जाता है, जिसे काम के प्रमाण को पुनः किए बिना बदला नहीं जा सकता। सबसे लम्बी चेन न सिर्फ इवेंट्स की श्रृंखला का प्रमाण देती है बल्कि वह प्रमाण भी देती है जो सीपीयू पावर के सबसे बड़े पूल से आया हो। जब तक ज़्यादातर सीपीयू पावर को नोड्स के द्वारा नियन्त्रित किया जाता है, जो नेटवर्क को अटैक करने के लिए कोऑपरेट नहीं करता, वे सबसे लम्बी चेन बनाते हैं और अटैकर्स को नियन्त्रित कर लेते हैं। नेटवर्क को न्यूनतम संरचना की ज़रूरत होती है। मैसेज को सबसे अच्छे प्रयास के आधार पर ब्रॉडकास्ट किया जाता है और नोड्स नेटवर्क को छोट कर फिर से इसके साथ जुड़ सकती हैं, इस तरह उनके जाने के प्रमाण के रूप से सबसे लम्बी प्रूफ-ऑफ-वर्क चेन को स्वीकार कर सकती हैं।

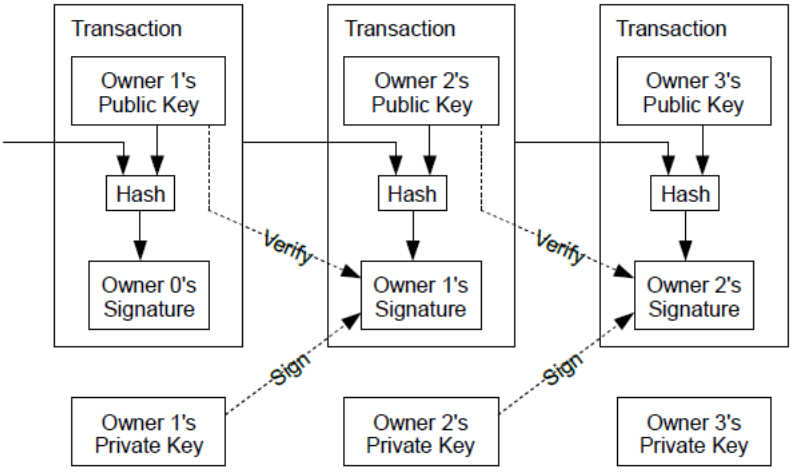
1. परिचय

इंटरनेट पर कॉमर्स, इलेक्ट्रोनिक भुगतान को प्रसंस्कृति करने के लिए भरोसेमंद थर्ड पार्टी के रूप में काम करने वाले वित्तीय संस्थान पर लगभग पूर्णतः निर्भर हो गया है। हालांकि यह सिस्टम ज़्यादातर लेनदेनों के लिए पर्याप्त हे, फिर भी इसे भरोसे पर आधारित मॉडल की कमज़ारी से नुकसान होता है। पूरी तरह नॉन-रिवर्सिबल लेनदेन वास्तव में संभव नहीं है, चूंकि वित्तीय संस्थान विवादों में मध्यस्थता से बच नहीं सकते। मध्यस्थता की लागत से लेनदेन की लागत बढ़ जाती है, लेनदेन का न्यूनतम व्यवहारिक आकार सीमित हो जाता है, तथा छोटे कैज़ुअल लेनदेन की संभावना कम हो जाती है। तथा नॉन-रिवर्सिबल सेवाओं के लिए नॉन-रिवर्सिबल भुगतान करने हेतु क्षमता के नुकसान में भारी लागत आती है। रिवर्सल की संभावना के साथ भरोसा की ज़रूरत बढ़ती है। मर्चेन्ट्स को अपने उपभोक्ताओं से सावधान रहना चाहिए, उनसे ज़रूरत से ज़्यादा जानकारी जुटानी चाहिए। धोखाधड़ी की सीमित मात्रा को **अनिवार्य** माना जाता है। भौतिक मुद्रा का उपयोग कर इस लागत और भुगतान की समस्याओं को व्यक्तिगत रूप से रोका जा सकता है, लेकिन ऐसी कोई प्रणाली मौजूद नहीं है जो एक भरोसेमंद पार्टी के बिना संचार चैनल पर भुगतान करने में सक्षम हो।

इसके लिए भरोसे के बजाए क्रिप्टोग्राफिक प्रमाण पर आधारित इलेक्ट्रोनिक भुगतान सिस्टम की आवश्यकता है, ताकि दो इच्छुक पार्टियां सीधे एक दूसरे के साथ लेनदेन कर सकें और इसमें भरोसेमंद थर्ड पार्टी की ज़रूरत न हो। लेनदेन जिन्हें रिवर्स करना व्यवहारिक नहीं है, वे विक्रेता को धोखाधड़ी से सुरक्षित रखते हैं, तथा खरीददार की सुरक्षा के लिए रूटीन एस्क्रो प्रणाली को आसानी से लागू किया जा सकता है। इस पेपर में हम पियर-टू-पियर टाईमस्टैम्प सर्वर के उपयोग द्वारा दोहरे खर्च की समस्या का समाधान लेकर आए हैं, जो लेनदेन के क्रम का कम्प्युटेशन प्रमाण उत्पन्न करता है। यह सिस्टम तब तक सुरक्षित है जब तक ऑनेस्ट नोड्स सामुहिक रूप से, अटैकर नोड्स के समूह की तुलना में अधिक सीपीयू पावर को नियन्त्रित करते हैं।

2- लेनदेन

हम इलेक्ट्रोनिक कॉयन को डिजिटल सिग्नेचर्स के चेन के रूप में परिभाषित करते हैं। हर मालिक पिछले लेनदेन पर हैश को डिजिटल रूप से साईन कर अगले मालिक को कॉयन स्थान्तरित करता है, इसके बाद अगले मालिक के पब्लिक की तक पहुंचता है और इसे कॉयन के अंत तक शामिल किया जाता है। भुगतान करने वाला स्वामित्व की श्रृंखला को सत्यापित करने के लिए सिग्नेचर को सत्यापित कर सकता है।

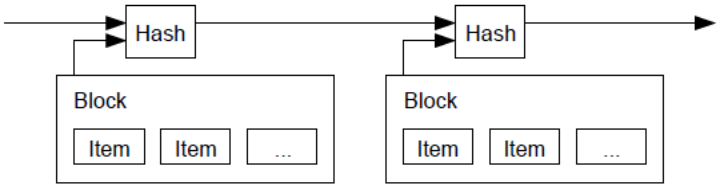


निश्चित रूप से समस्या यह है कि भुगतान करने वाला व्यक्ति इस बात को सत्यापित नहीं कर सकता है कि मालिकों में से एक ने कायॅन को दोहरा खर्च नहीं किया। इसका समाधान यह है कि तीसरी केन्द्रीय ऑथोरिटी या मिंट को शामिल किया जाए जो हर लेनदेन को दोहरे खर्च के लिए जांच करे। हर लेनदेन के बाद कॉयन को नया कॉयन जारी करने के लिए मिंट को लौटाया जाता है, और केवल मिंट से जारी किए गए कॉयन ही भरोसेमंद होते हैं कि इन्हें दोहरा खर्च नहीं किया गया है। इस समस्या का समाधान यह है कि पूरा मनी सिस्टम मिंट चलाने वाली कंपनी पर निर्भर करता है, और हर लेनदेन को बैंक की तरह इनसे होकर गुज़रना पड़ता है।

हमें ऐसा तरीके की आवश्यकता है जिसके द्वारा भुगतानकर्ता यह जान सके कि पिछले मालिक ने किसी पिछले लेनदेन पर साईन नहीं किए हैं। हमारे इस प्रयोजन के लिए सबसे पहला लेनदेन वह है, जिसकी गणना की गई है। इसलिए हम दोहरे खर्च के लिए बार में किए गए प्रयास की परवाह नहीं करते। लेनदेन की अनुपस्थिति की पुष्टि करने का एकमात्र तरीका यह है कि सभी लेनदेनों के बारे में जानकारी हो। मिंट आधारित मॉडल में मिंट सभी लेनदेनों से अवगत था और उसी ने फैसला लिया कि कौनसा लेनदेन पहले हुआ। भरोसेमंद पार्टी के बिना इसे हासिल करने के लिए, लेनदेन की सार्वजनिक घोषणा की जानी चाहिए। और हमें ऐसे सिस्टम की ज़रूरत है जहां प्रतिभागी क्रम की हर एक हिस्ट्री पर सहमत हों, जो उन्हें मिला है। भुगतानकर्ता को हर लेनदेन के समय ऐसे प्रमाण की ज़रूरत है, ज़्यादातर नोड्स इस बात से सहमत हैं कि जब यह पहले प्राप्त हुआ।

3- टाईमस्टैम्प सर्वर

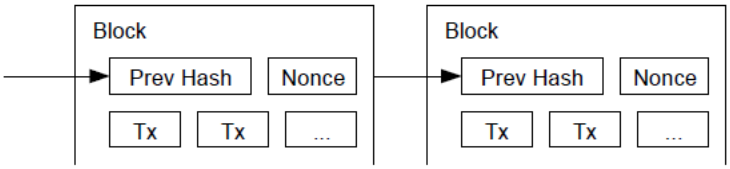
हम जो समाधान प्रस्तावित करते हैं, उसकी शुरूआत टाईमस्टैम्प सर्वर के साथ होती है। टाईमस्टैम्प सर्वर, टाईमस्टैम्प किए जाने वाले आइटम के ब्लॉक का हैश लेकर काम करता है और हैश को उस तरह से व्यापक रूप से प्रकाशित करता है, जैसे अखबार या यूज़नेट पोस्ट (2-5) में किया जाता है। टाईमस्टैम्प प्रमाणित करता है कि हैश को प्राप्त करने के लिए डेटा उपलब्ध हो। हर टाईमस्टैम्प में इसके हैश में पिछली टाईमस्टैम्प शामिल होती है, जो चेन बनाती है, और हर अतिरिक्त टाईमस्टैम्प इससे पिछले की पुष्टि करती है।



4- काम का प्रमाण

पियर-टू-पियर आधार पर वितरित टाईमस्टैम्प सर्वर को लागू करेन के लिए हमें अखबार या यूज़नेट पोस्ट के बजाए एडम बैक के हैशकैश (6) की तरह प्रूफ-ऑफ-वर्क सिस्टम का उपयोग करना होगा। प्रूफ-ऑफ-वर्क में हैश किए जाने पर वैल्यू की स्कैनिंग शामिल है, जैसे SHA-256 के साथ। हैश की शुरूआत ज़ीरो बिट्स के नंबर के साथ होती है। औसत कार्य ज़ीरो बिट्स के नंबर में घातांक की तरह होता है और इसे सिंगल हैश में निष्पादित कर सत्यापित किया जा सकता है।

टाईमस्टैम्प नेटवर्क के लिए हम ब्लॉक में नॉनस को बढ़ाकर तब तक प्रूफ-ऑफ-वर्क को लागू करते हैं, जब तक वो वैल्यू न मिल जाए जो ब्लॉक के हैश को आवश्यक ज़ीरो बिट्स प्रदान करे। जब सीपीयू प्रयास को प्रूफ-ऑफ-वर्क के लिए विस्तारित किया जाता है, काम को दोबारा किए बिना ब्लॉक को बदला नहीं जा सकता। बाद में ब्लॉक को इसके बाद चेन में लगाया जाता है, ब्लॉक को बदलने के कार्य में सभी ब्लॉक्स को फिर से इसके पीछे लगाना होता है। .



प्रूफ-ऑफ-वर्क ज़्यादातर फैसलों में प्रतिनिधित्व को निर्धारित करने की समस्या हल करता है। अगर ज़्यादातर मामले एक-आईपी-अड्रैस-एक-वोट पर आधारित हों तो इसे किसी ऐसे व्यक्ति द्वारा उलटा जा सकता है जो कई आईपी आवंटित करने में सक्षम हो। प्रूफ-ऑफ-वर्क निश्चित रूप से एक-सीपीयू-एक-वोट है। सबसे लम्बी चेन द्वारा दर्शाए गए ज़्यादातर फैसले, जिसमें सबसे ज़्यादा प्रूफ-ऑफ-वर्क को निवेश किया जाता है। अगर ज़्यादातर सीपीयू पावर को ऑनेस्ट नोड्स द्वारा नियन्त्रित किया जाता है जो ऑनेस्ट चेन तेज़ी से बढ़ेगी और प्रतिस्पर्धी चेन को पीछे छोड़ देगी। पिछले ब्लॉक को संशोधित करने के लिए अटैकर को ब्लॉक एवं इसके बाद से सभी ब्लॉक्स के प्रूफ-ऑफ-वर्क को फिर से करना होगा और फिर ऑनेस्ट नोड्स के काम के साथ तालमेल बनाना होगा। हम बाद में बताएंगे कि बाद के ब्लॉक्स शामिल करने से धीमे अटैकर के पकड़ में आने की संभावना तेज़ी से कम हो जाती है।

समय के साथ रनिंग नोड्स में हार्डवेयर स्पीड बढ़ाने हेतु प्रतिपूर्ति के लिए प्रूफ-ऑफ-वर्क की मुश्किल का निर्धारण प्रति घण्टे ब्लॉक्स की औसत संख्या का औसत लक्ष्य बनाकर किया जाता है। अगर ये तेज़ी से जनरेट होते हैं, तो मुश्किल बढ़ जाती है।

5- नेटवर्क

नेटवर्क चलाने के लिए चरणः

- नए लेनदेन को सभी नोड्स को ब्रॉडकास्ट किया जाता है।
- हर नोड नए लेनदेनों को एक ब्लॉक में इकट्ठा करता है।
- हर नोड इसके ब्लॉक के लिए मुश्किल प्रूफ-ऑफ-वर्क को खोजने पर काम करता है।
- जब एक नोड को प्रूफ-ऑफ-वर्क मिल जाता है, यह सभी नोड्स को ब्रॉडकास्ट करता है।
- नोड्स ब्लॉक को तभी स्वीकार करते हैं अगर इसमें होने वाले सभी लेनदेन वैद्य हों और पहले से खर्च न हुए हों।
- नोड्स चेन में अगले ब्लॉक के निर्माण पर काम करके ब्लॉक की स्वीकार्यता की अभिव्यक्ति करते हैं, इसके लिए वे पिछले हैश की तरह स्वीकार किए गए ब्लॉक्स के हैश का उपयोग करते हैं।

नोड्स हमेशा सबसे लम्बी चेन को सही मानते हैं और इसे विस्तारित करते रहने के लिए काम करते हैं। अगर दो नोड्स, एक ही समय में अगले ब्लॉक के विभिन्न वर्ज़न्स को ब्रॉडकास्ट करते हैं, तो हो सकता है कि कुछ नोड्स एक या अन्य को प्राप्त कर सकते हैं। ऐसे मामले में, वे सबसे पहले प्राप्त होने वाले पर काम करते हैं और अगर यह लम्बा हो जाए तो दूसरी शाखा को बचा लेते हैं। अगला प्रूफ-ऑफ-वर्क मिलने पर बंधन (टाई) टूट जाएगा और एक शाखा लम्बी हो जाएगी; नोड्स जो अन्य शाखा पर काम कर रहे थे, वे लम्बी वाली शाखा पर चले जाएंगे।

ज़रूरी नहीं कि नए लेनदेन ब्रॉडकास्ट सभी नोड्स तक पहुंचे। जब वे कई नोड्स तक पहुंचते हैं, वे लम्बे से पहले वाले ब्लॉक पर आ जाते हैं। ब्लॉक ब्रॉडकास्ट ड्रॉप हुए मैसेज को भी प्राप्त करते हैं। अगर किसी मोड को ब्लॉक नहीं मिलता, तो यह इसके लिए रिक्वेस्ट करेगा, जब इसका अगला ब्लॉक मिल जाएगा तो चूके हुए ब्लॉक का पता चल जाएगा।

6- इन्सेन्टिव

आमतौर पर ब्लॉक में पहला लेनदेन विशेष लेनदेन होता है, जो ब्लॉक के क्रिएटर द्वारा प्राप्त किए गए नए कॉयन से शुरू होता है। इससे नेटवर्क को सपोर्ट करने के लिए नोड्स के लिए इन्सेन्टिव मिलता है। यह शुरूआत में कॉयन्स को सर्कुलेशन में लाने का तरीका है, चूंकि इन्हें जारी करने के लिए कोई केंद्रीय ऑथोरिटी नहीं है। नए कॉयन्स को लगातार शामिल करना, सोने के खनिकों द्वारा संसाधनों को विस्तारित करने के लिए सोने को सर्कुलेशन में शामिल करने की तरह है। हमारे मामले में यह सीपीयू टाईम और विद्युत है, जिसे विस्तारित किया गया है।

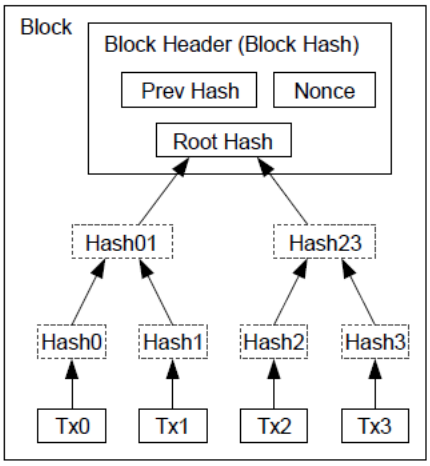
इन्सेन्टिव को लेनदेन शुल्क के साथ वित्तपोषित किया जा सकता है। अगर लेनदेन का आउटपुट मूल्य इनपुट मूल्य से कम हो तो लेनदेन शुल्क का अंतर लेनदेन वाले ब्लॉक के इन्सेन्टिव मूल्य में शामिल किया जाता है। जब कॉयन्स की पहले से निर्धारित संख्या सर्कुलेशन में आ जाती है, तक इन्सेन्टिव पूरी तरह से लेनदेन शुल्क में बदला जा सकता है और पूरी तरह से मुद्रास्फीती से मुक्त् हो सकता है।

इन्सेन्टिव नोड्स को ऑनेस्ट (ईमानदार) बने रहने के लिए प्रोत्साहित करते हैं। अगर लालची अटैकर ऑनेस्ट नोड्स की तुलना में अधिक सीपीयू पावर को असेम्बल करने में सक्षम हो तो उसे विकल्प चुनना होगा कि वह अपने भुगतान को वापस चुराकर लोगों को धोखा देने के लिए इसका इस्तेमाल करे या नए कॉयन्स जनरेट करने के लिए इसका इस्तेमाल करे। उसे नियमों के अनुसार खेलते हुए अधिक मुनाफ़ा कमाना चाहिए, ऐसे नियम उसके सिस्टम का कमज़ोर बनाने के बजाए उसे नए कॉयन्स जनरेट करने के लिए मदद करते हैं।

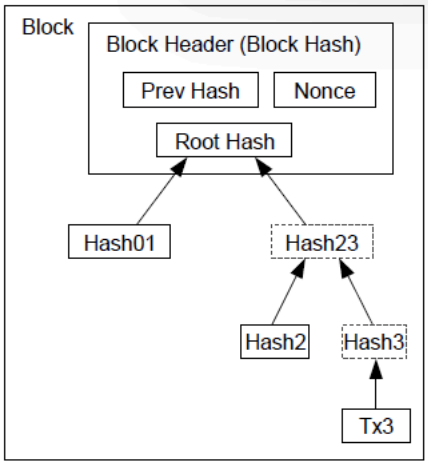
7- डिस्क स्पेस को पुनः प्राप्त करना

जब कॉयन में नया लेनदेन पर्याप्त ब्लॉक्स के नीचे जाए, तो पिछले खर्च किए गए लेनदेन को डिस्कार्ड कर डिस्क स्पेस को बचाया जा सकता है। ब्लॉक के हैश को तोड़े बिना ऐसा करने के लिए लेनदेन को मर्कल ट्री में हैश किया जाता है (7)(2)(5), ऐसा ब्लॉक के हैश में शामिल रूट के साथ किया जाता है। इसके बाद पुराने ब्लॉक के पेड़ की शाखाओं को काट कर कॉम्पैक्ट किया जा सकता है। इंटीरियर हैश को स्टोर करने की

ज़रूरत नहीं होती।



Transactions Hashed in a Merkle Tree

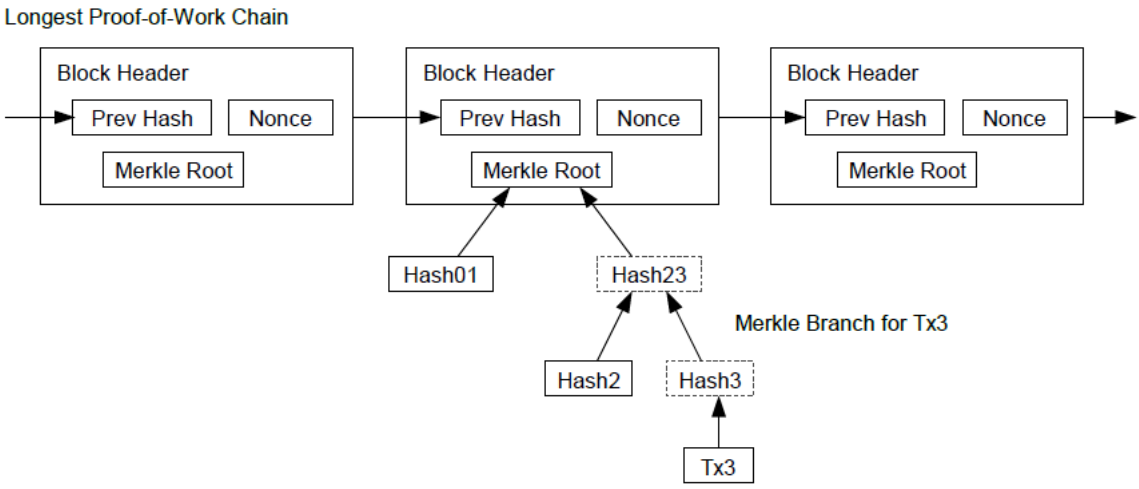


After Pruning Tx0-2 from the Block

बिना लेनदेन का ब्लॉक हैडर तकरीबन 80 बाईट्स का होगा। अगर मान लें कि हर 10 मिनट में ब्लॉक जनरेट होते हैं तो सालाना यह संख्या होगी 80 बाईट्स * 6 * 24 * 365 = 4.2MB । 2008 में 2जीबी रैम के कम्प्यूटर सिस्टम बेचा जाता है, मूरे के नियम के अनुसार मौजूदा विकास दर 1.2 जीबी सालाना है, ऐसे में स्टोरेज की समस्या नहीं होगी अगर ब्लॉक हडर्स को मैमोरी में रखा जाए।

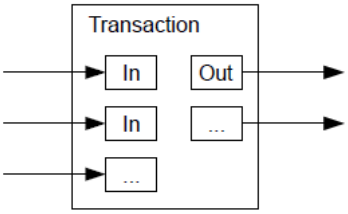
8- पेमेन्ट के वैरिफिकेशन को सुगम बनाना

पूरे नेटवर्क मोड को चलाए बिना पेमेंट को वैरीफाय करना संभव है। इसके लिए यूज़र को सबसे लम्बे प्रूफ-ऑफ-वर्क चेन के ब्लॉक हैडर्स की कॉपी रखनी होगी, वह नेटवर्क नोड्स की जानकारी पाकर ऐसा कर सकता है। जब उसे लगे कि उसके पास सबसे लम्बी चेन है और लेनदेन को टाईमस्टैम्प किए गए ब्लॉक के साथ लिंक करने वाली मर्कल शाखा मिल गई है। वह अपने आप लेनदेन की जांच नहीं कर सकता, लेकिन इसे चेन में लिंक कर अपने द्वारा स्वीकार किए गए नोड को देख सकता है। इसके बाद शामिल किए गए ब्लॉक्स इस बात की पुष्टि करते हैं कि नेटवर्क ने इसे स्वीकार कर लिया है।



वैरीफिकेशन तब तक भरोसेमंद है जब तक ऑनेस्ट नोड्स नेटवर्क को नियन्त्रित करते हैं, लेकिन यह अधिक संवेदनशील होजाता है अगर नेटवर्क को अटैकर द्वारा नियन्त्रित कर लिया जाए। जब नेटवर्क नोड्स अपने लिए लेनदेन को वैरीफाय कर सकते हैं, यह आसान तरीका अपनाकर अटैकर नेटवर्क पर नियन्त्रण बनाए रख सकता है और धोखा दे सकता है। इससे सुरक्षा का एक तरीका यह है कि नेटवर्क नोड्स से एलर्ट को स्वीकार किया जाए जब वे अवैद्य ब्लॉक को डिटेक्ट करें, ताकि यूज़र पूरे ब्लॉक को डाउनलोड कर विसंगति की पुष्टि कर सके और एलर्ट किए गए लेनदेन पर ध्यान दे सके। जिन कारोबारों को लगातार पेमेंट मिलते हैं, वे संभवतया अधिक स्वतन्त्र सुरक्षा एवं त्वरित वैरिफिकेशन के लिए अपने खुद के नोड्स संचालित करना चाहते हैं।

9- विभाजन मूल्य को संयोजित करना

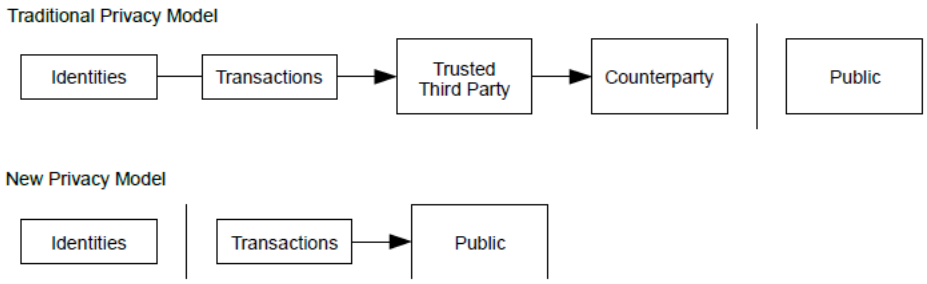


हालांकि कॉयन्स को व्यक्तिगत रूप से हैण्डल करना संभव है, लेकिन ट्रांसफर के हर सेंट के लिए लेनदेन को अलग करना अव्यवहारिक हो सकता है। वैल्यू को विभाजित और संयुक्त करने के लिए लेनदेनों में कई इनपुट और आउटपुट शामिल किए जाते हैं। आमतौर पर बड़े पिछले लेनदेन से एक इनपुट होता है या छोटी राशियां को मिलकार कई इनपुट बनते हैं। ज़्यादातर दो आउटपुट मेंः एक पेमेंट के लिए और एक शेष राशि लौटाने के लिए होता है, अगर कोई है।

इस बात पर ध्यान दिया जाना चाहिए कि फैन-आउट, जहां एक लेनदेन कई लेनदेनों पर निर्भर करता है और ये लेनदेन कई और पर निर्भर करते हैं, यहां यह समस्या नहीं है। लेनदेन की हिस्ट्री की सम्पूर्ण स्टैण्डअलोन कॉपी निकालना कभी ज़रूरी नहीं होता।

10. गोपनीयता

पारम्परिक बैंकिंग मॉडल अन्य पार्टियों या भरोसेमंद थर्ड पार्टी के लिए जानकारी के एक्सेस को सीमित कर गोपनीयता का उच्चतम स्तर हासिल करता है। सभी लेनदेनों की सार्वजनिक घोषणा इस तरीके को रोकती है, लेकिन अन्य स्थान पर जानकारी के प्रभाव को तोड़कर और पब्लिक की को अनाम बना कर गोपनीयता को बनाए रखा जा सकता है। जनता देख सकती है कि कोई एक राशि को किसी दूसरे व्यक्ति को भेज रहा है ,लेकिन लेनदेन को किसी के साथ लिंक नहीं किया जा रहा। यह स्टॉक एक्सचेंज द्वारा जारी जानकारी की तरह है, जहां व्यक्तिगत ट्रेड का समय और साइज़, 'टेप' को सार्वजनिक बनाया जाता है, लेकिन यह नहीं बताया जाता कि पार्टियां कौनसी थीं।



अतिरिक्त फायरवॉल की तरह, नया की पेयर हर लेनदेन के लिए काम में लिया जाना चाहिए, ताकि इसे कॉमन मालिक के साथ लिंक किया जा सके। कुछ लिंकिंग को मल्टी-इनपुट लेनदेनों के साथ रोकना संभव है, जो निश्चित रूप से बताते हैं कि इनपुट उसी मालिक के थे। जोखिम यह है कि अगर की का पता चल जाए तो लिंकिंग के द्वारा इसी मालिक के अन्य लेनदेनों की जानकारी भी मिल जाती है।

11- गणना

मान लीजिए कि एक अटैकर ऑनेस्ट चेन की तुलना में तेज़ी से वैकल्पिक चेन जनरेट करने की कोशिश कर रहा है। अगर ऐसा हो भी जाए, तो यह सिस्टम में अनिवार्य बदलाव नहीं आते, जैसे थिन एयर से वैल्यू क्रिएट करना या ऐसा धन प्राप्त करना जो कभी भी अटैकर का नहीं था। नोड्स अवैद्य लेनदेन को पेमेंट के रूप में स्वीकार नहीं करते और ऑनेस्ट नोड्स कभी भी उनमें मौजूद ब्लॉक को स्वीकार नहीं करते। एक अटैकर अपने लेनदेन को बदलकर हाल ही में खर्च किए गए पैसे को वापस पाने की कोशिश कर सकता है।

ऑनेस्ट चेन और अटैकर चेन के बीच की रेस को बाइनोमियल रैंडम वॉक से परिभाषित किया जाता है। सफलता घटना एक ऑनेस्ट चेन है, जिसे एक ब्लॉक से विस्तारित किया जाता है, जिससे यह 1 की बढ़त ले लेता है। इसी तरह असफल होने पर अटैकर की चेन एक ब्लॉक से विस्तारित हो जाती है और अंतर माइनस 1 हो जाता है।

अटैकर द्वारा इससे उबरने की संभावना ठीक गैम्बलर की तरह होती है। मान लीजिए एक गैम्बलर ने असीमित क्रेडिट लिया है तो वह ब्रेक-ईवन तक पहुंचने के लिए असंख्य बार ट्रायल लेता है। हम ब्रेक-ईवन तक पहुंचने की संभावना या अटैकर द्वारा ऑनेस्ट चेन तक पहुंचने की संभावना की गणना निम्नानुसार कर सकते हैं:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

मान लीजिए पी क्यू से अधिक है, तो संभावना तेज़ी से कम होती है क्योंकि अटैकर के पास ब्लॉक्स की संख्या बढ़ती है। अपने खिलाफ़ बाधाओं के साथ अगर उसकी किस्मत अच्छी न हो तो उसके पीछे छूटने की संभावना बढ़ती जाती है।

अब हम इस बात पर विचार करते हैं कि नए लेनदेन के प्राप्तकर्ता को यह सुनिश्चित करने से पहले इंतज़ार करना पड़ता है कि प्रेषक लेनदेन को बदल नहीं सकता। हम मान लेते हैं कि प्रेषक एक अटैकर है जो प्राप्तकर्ता को विश्वास दिलाना चाहता है कि उसने कुछ समय के लिए भुगतान किया है, फिर कुछ समय बीतने के बाद भुगतान को बदल देता है। ऐसा होने पर प्राप्तकर्ता को सतर्क किया जाएगा, लेकिन प्रेषक को उम्मीद है कि तब तक बहुत देर हो चुकी होगी।

प्राप्तकर्ता नया की पेयर जनरेट करता है और साइनिंग से ठीक पहले पब्लिक की को प्रेषक को भेजता है। इससे प्रेषक समय से पहले ब्लॉक की सीरीज़ तैयार नहीं करता, जब तक कि उसकी किस्मत इतनी अच्छी न हो कि वह आगे न निकल जाए, फिर वह लेनदेन को निष्पादित करता है। एक बार लेनदेन भेजे जाने के बाद, बेईमान प्रेषक अपने लेनदेन के वैकल्पिक संस्करण वाली समानांतर श्रंखला पर गुप्त रूप से काम करना शुरू कर देता है।

प्राप्तकर्ता जब तक प्रतीक्षा करता है जब तक कि लेनदेन को ब्लॉक में जोड़ नहीं दिया जाता। और उसके बाद ज़ैड ब्लॉक लिंक नहीं हो जाते। उसे अटैकर द्वारा की गई प्रगति के बारे में जानकारी नहीं होती, लेकिन मान लीजिए कि ऑनेस्ट ब्लॉक ने प्रति ब्लॉक अपेक्षित समय लिया, अटैकर की संभावित प्रगति अपेक्षित मूल्य के साथ पॉइसन वितरण होगीः

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12 निष्कर्ष

हम भरोसे के बिना इलेक्ट्रोनिक लेनदेन के लिए एक सिस्टम की प्रस्तावना लेकर आए हैं। हमने डिजिटल सिग्नेचर्स से बने कॉयन्स के आम फ्रेमवर्क के साथ शुरूअत की, जो स्वामित्व का नियन्त्रण देता है। लेकिन दोहरे खर्च को रोके बिना अपूर्ण है। इसे हल करने के लिए हम प्रूफ-ऑफ-वर्क का उपयोग कर पियर-टू-पियर नेटवर्क की प्रस्तावना देते हैं। इसमें लेनदेनों की पब्लिक हिस्ट्री को रिकॉर्ड किया जाता है जो अटैकर के लिए अव्यवहारिक बन जाती है, अगर ऑनेस्ट नोड्स ज़्यादातर सीपीयू पावर को नियन्त्रित कर लें। नेटवर्क अपनी असंरचित सादगी में मजबूत है। नोड्स हल्के तालमेल में काम करते हैं। इन्हें पहचाने जाने की ज़रूरत नहीं होती, चूंकि मैसेज किसी विशेष स्थान पर नहीं जाते और इन्हें सर्वश्रेष्ठ प्रयास के आधार पर डिलीवर करना होता है। नोड्स नेटवर्क को छोड़

कर इसमें फिर से शामिल हो सकते हैं और प्रूफ-ऑफ-वर्क चेन को उस प्रमाण के रूप में स्वीकार करते हैं, जो हो चुका है। वे अपनी सीपीयू पावर के साथर वैद्य ब्लॉक्स को स्वीकार करते हैं और अवैद्य ब्लॉक्स को अस्वीकार करते हैं। आवश्यक नियमों और इन्सेंटिव्स को सहमति प्रणाली के साथ लागू किया जा सकता है।

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.