Translated in Hindi from bitcoin.org/bitcoin.pdf
By PRANEET JAIN PSRP.ROOT[at]protonmail[dot]com

बिटकॉइन - एक सहकर्मी-से-सहकर्मी इलेक्ट्रॉनिक मुद्रा तंत्र

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

सार। इलेक्ट्रॉनिक मुद्रा का सहकर्मी-से-सहकर्मी के लिए शुद्ध संस्करण, ऑनलइन भुगतान को एक पार्टी से दूसरी को बिना किसी वित्तीय संस्थान के बिना भेजने की अनुमति देगा। डिजिटल हस्ताक्षार समाधान का एक हिस्सा हैं, लेकिन अगर दोहरे-खर्च को रोकने के लिए फिर भी किसी विश्वसनीय तीसरी पार्टी की ज़रूरत पड़े तो डिजिटल हस्ताक्षार का मुख्य लाभ खो जाता है। हम सहकर्मी-से-सहकर्मी नेटवर्क का उपयोग कर दोहरे खर्च की समस्या का समाधान प्रस्तावित करते हैं। यह नेटवर्क लेनदेन को समय-छाप करने के लिए, हैश आधारित कार्य-का-प्रमाण प्रक्रिया की एक निरंतर श्रृंखला में हैशिंग करता है, जिस से एक रिकॉर्ड बनता है, रिकॉर्ड को बिना कार्य-का-प्रमाण प्रक्रिया को फिर से दोहराये बिना बदला नहीं जा सकता। सबसे लम्बी श्रृंखला न केवल देखि गयी घटनाओं के अनुक्रम के प्रमाण के रूप में कार्‌य करती हैं, बल्कि सबूत हैं कि ये सीपीयु ऊर्जा के सबसे बड़े कुंड में से आयी है। जब तक सीपीयु की अधिकाँश ऊर्जा उन ग्रंथियों द्वारा नियंत्रित की जाती है जो नेटवर्क पर हमला करने में सहयोग नहीं कर रही, वे ग्रंथिया सबसे लम्बी श्रृंखला उत्पन्न करेंगी और नेटवर्क के हमलावरों को पीछे छोड़ देंगी। नेटवर्क को स्वयं न्यूनतम संरचना की आवश्यकता होती है। संदेशो को एक सर्वोत्तम प्रयास के आधार पर प्रसारित किया जाता है, ग्रंथियां नेटवर्क अपनी मर्ज़ी से छोड़ सकती हैं, और उनकी अनुपस्थिति में क्या हुआ इसका सबूत सबसे लम्बी काम-का-प्रमाण आधारित शृंखला को स्वीकार कर फिर से शामिल हो सकती है।

१. परिचय

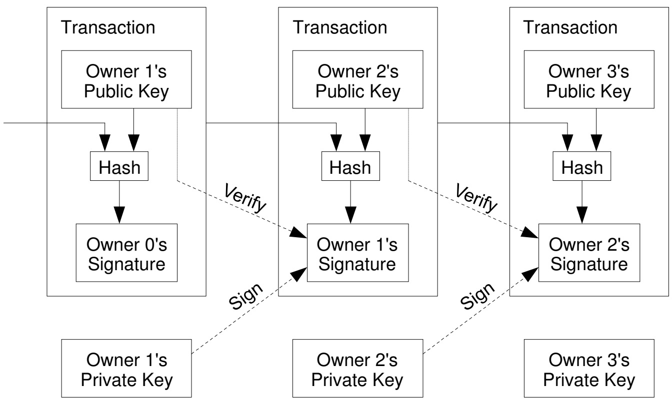
इंटरनेट पर व्यापार लगभग पूर्ण रूप से उन वित्तीय संस्थानों जो कि इलेक्ट्रॉनिक भुगतान को संचालित करने के लिए भरोसेमंद तृतीय पार्टी हैं, उन पर आश्रित है। हाँलाकि यह तंत्र अधिकाँश लेनदेन के लिए पर्याप्त रूप से काम करता है, फिर भी यह विश्वास आधारित मॉडल की अंतर्निर्हित कमज़ोरियों से ग्रस्त है। पूरी तरह से गैर-प्रतिवर्तित लेनदेन वास्तव में संभव नहीं है, क्यूँकि वित्तीय संस्थान विवादों में मध्यस्थता करने से नहीं बच सकते हैं। मध्यस्थता की लागत लेनदेन की लागत को बढाती है, न्यूनतम व्यवहारिक लेनदेन आकर को सीमित करती है और छोटे आकस्मिक लेनदेन के लिए संभावनाओं को खत्म कर देती है, और गैर-प्रतिवर्ती सेवाओं के लिए गैर-प्रतिवर्ती भुगतान करने की क्षमता में कमी की कीमत व्यापक होती

है। प्रतिवर्तन की संभावना की वजह से, भरोसे की ज़रूरत बढ़ती है। व्यापारियों को अपने ग्राहको से होशियार रहना चाहिए, ज़रूरत से ज़्यादा जानकारी के लिए उन्हें परेशान करना चाहिए। एक निश्चित प्रतिशत धोखाधड़ी को नहीं ताला जा सकता, यह मान्य है। इन लागत और भुगतान की अनिश्चितताओं को स्वयं भौतिक मुद्रा का उपयोग करके ताला जा सकता है, लेकिन संचार चैनल पर बिना भरोसेमंद पार्टी के भुगतान की कोई क्रियाविधि नहीं है।

ज़रूरत क्या है फिर, एक इलेक्ट्रॉनिक भुगतान तंत्र जो विश्वास की बजाय क्रिप्टोग्राफ़िक सबुत पर आधारित है, यह बिना किसी भरोसेमंद तीसरी पार्टी के बिना दो इच्छुक पार्टियों को सीधे लेन-देन में सक्षम करता है। लेन-देन का हिसाब जिसे प्रतिवर्तित करना असंभव है वह विक्रेताओं को धोखाधड़ी से बचाएँगे, और खरीददारों को बचाने के लिए सामान्य एस्क्रो प्रणाली को आसानी से लागु किया जा सकता है। इस पत्र में, सहकर्मी-से-सहकर्मी वितरित समयछाप सर्वर द्वारा लेन-देन के कालानुक्रमिक क्रम का प्रमाण सहित हिसाब बना कर हम दोहरे-खर्च की समस्या के समाधान का प्रस्ताव करते हैं। जब तक ईमानदार ग्रंथियां हमलावर ग्रंथियों के सहयोगी समूह से ज़्यादा सीपीयु ऊर्जा नियंत्रित करती हैं तब तक यह तंत्र सुरक्षित है।

२. लेनदेन

हम इलेक्ट्रॉनिक सिक्के को डिजिटल हस्ताक्षर की श्रृंखला के रूप में परिभाषित करते हैं। प्रत्येक सिक्के का मालिक पिछले लेनदेन के हैश और अगले मालिक की सार्वजनिक कुंजी को डिजिटल हस्ताक्षर करके और सिक्के के अंत में जोड़ कर स्थानांतरण कर सकता है। प्राप्तकर्ता मालिकाना श्रृंखला को सत्यापित करने के लिए हस्ताक्षरों की जांच कर सकता है।



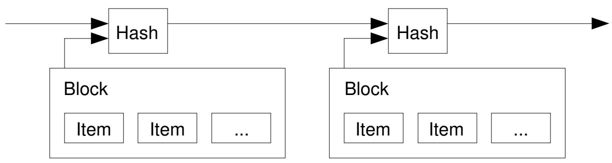
निश्चित रूप से यह समस्या है कि भुगतान पाने वाला नहीं जांच पाएगा कि मालिकों में से एक ने सिक्के का दोहरा खर्च नहीं किया है। एक साधारण समाधान यह है कि एक विश्वसनीय केंद्रीय प्राधिकरण या टकसाल को लाना जो हर लेनदेन के दोहरे खर्च की जांच करें। प्रत्येक लेन-देन के बाद, टकसाल द्वारा नया सिक्का जारी करने हेतु पुराना सिक्का टकसाल में जमा होना चाहिए तथा टकसाल से जारी किये सिक्कों पर ही दोहरे-खर्च ना करने का भरोसा किया जायेगा। इस समाधान के साथ यह समस्या है कि संपूर्ण धन

प्रणाली तंत्र का भाग्य टकसाल चलाने वाली कंपनी पर निर्भर करता है, हर लेन-देन का माध्यम वही है, एक बैंक की तरह।

हमे भुगतान पाने वालों को यह जानने के लिए कि पिछले मालिक ने किसी भी पुराने लेन-देन पर हस्ताक्षर नहीं किये हैं, एक रास्ता चाहिए। हमारे उद्देश्यों के लिए, सबसे पहला लेनदेन ही मायने रखता है, इसलिए हम बाद में दोहरे-खर्च लेनदेन के प्रयासों के बारे में परवाह नहीं करते। एक लेनदेन की अनुपस्थिति की पुष्टि करने का एकमात्र तरीका सभी लेनदेन के बारे में जागरूक होना है। टकसाल आधारित मॉडल में, टकसाल को सभी लेनदेन की जानकारी थी, पहला लेनदेन उसी आधार पर तय कर लिया गया। एक विश्वसनीय पार्टी के बिना इसे पूर्ण करने के लिए सभी लेनदेन सार्वजनिक रूप से घोषित किया जाना चाहिए [१] और हमें प्रतिभागियों के उस आदेश के एकल इतिहास, जिसमे उन्हें प्राप्त किया गया था की सहमति के लिए एक तंत्र चाहिए। भुगतान पाने वालों को इस बात का प्रमाण चाहिए कि प्रत्येक लेनदेन के समय, अधिकाँश ग्रन्थियाँ सहमत थी कि यह पहले प्राप्त हुआ।

३. समयछाप सर्वर

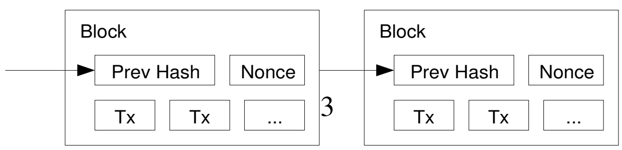
हमारे द्वारा प्रस्तावित समाधान एक समयछाप सर्वर से शुरू होता है। एक समयछाप सर्वर, वस्तुओं के ब्लाक का हैश जिसे समयछाप करना है उन्हें लेकर करता है तथा उन्हें अखबार या यूजनेट डाक की तरह व्यापक रूप से प्रकाशित करता है [२-५]। समयछाप प्रमाणित करता है कि डाटा का उस समय अस्तित्त्व था, ज़ाहिर है हैश में आने के लिए। प्रत्येक समयछाप हैश में पुराना समयछाप एक श्रृंखला बनाते हुए सम्मिलित करता है, एवं अतिरिक्त समयछाप पहले वालों को और मज़बुत बनाते हैं।



४. कार्य-का-प्रमाण

सहकर्मी-से-सहकर्मी के आधार पर वितरित समयछाप सर्वर को लागू करने के लिए, हमें अखबार या यूज़नेट पोस्ट के बजाय एडमबैक की हैशकैश [६] सामान कार्य-का-प्रमाण तंत्र उपयोग करना होगा। कार्य-का-प्रमाण एक हैश होती हुई निधि का अवलोकन करना है, जैसे कि SHA-२५६ हैश कई शुन्य बिट के साथ शुरु होता है। औसतन कार्य शुन्य बिट्स की संख्या में घातिय है और एकल हैश निष्पादित करके सत्यापित किया जा सकता है।

हमारे समयछाप नेटवर्क के लिए, हम कार्य-का-प्रमाण प्रक्रिया जब तक कि एक निधि, जो ब्लॉक के हैश को ज़रूरी शुन्य बिट्स ना दे, तब तक ब्लॉक में अस्थायी वृद्धि करके लागू करते हैं। एक बार सीपीयु का प्रयास कार्य-का-प्रमाण को संतुष्ट करने के लिए व्यय कर दिया तो ब्लॉक को बिना कार्य किये नहीं बदला जा सकता। जैसा कि सभी ब्लॉक एक के बाद एक श्रृंखला बना लेते हैं, तो एक ब्लॉक को बदलने के लिए उसके बाद के सभी ब्लॉकों को बदलना होगा।



कार्य-का-प्रमाण बहुमत आधारित निर्णय लेने में प्रतिनिधित्व का निर्धारण करने की समस्या को हल करता है। यदि बहुमत एक-आईपी-एड्रेस-एक-वोट पर आधारित होता, तो किसी के भी द्वारा बहुमत को कई आईपी आवंटित करके पलटा जा सकता था। कार्य-का-प्रमाण अनियार्य ही एक-सीपीयु-एक-वोट है। बहुमत के निर्णय को सब लम्बी श्रृंखला द्वारा दर्शाया जाता है, जिसमें अधिकतम कार्य-का-प्रमाण श्रम लगा होता है। यदि अधिकाँश सीपीयु ऊर्जा ईमानदार ग्रंथियों द्वारा नियंत्रित हैं तो इमानदार श्रृंखला सबसे तेज़ी से आगे बढ़ेंगी और किसी भी प्रतिस्पर्धा श्रृंखला को पीछे छोड़ देंगी। पिछले ब्लॉक को बदलने के लिए, हमलावर को ब्लॉक के कार्य-का-प्रमाण फिर से दोहराना होगा, उस ब्लॉक के बाद के सभी ब्लॉक का भी और फिर भी ईमानदार ग्रंथियों के काम को पार करना होगा। यह हम बाद में दिखाएंगे कि सुस्त हमलावर को पकड़ने की संभावना आगामी ब्लॉक में जुड़ने की वजह से कैसे तेज़ी से कम हो जाती है।

बढ़ी हुई हार्डवेयर की गति और चलती हुई ग्रंथियों की भिन्न-भिन्न रुचियों के लिए, कार्य-का-प्रमाण की कठिनाई सामान्य गति जो प्रति घंटे ब्लॉक की संख्या से निकलती है। अगर ब्लॉक बहुत तेज़ी से उत्पन्न होते हैं, तो कठिनाई बढ़ जाती है।

५. नेटवर्क

नेटवर्क चलाने के चरण इस प्रकार हैं:

a. नए लेनदेन सभी ग्रंथियों में प्रसारित किए जाते हैं।
b. प्रत्येक ग्रंथि एक ब्लॉक में नए लेनदेन एकत्र करती है।
c. प्रत्येक ग्रंथि अपने ब्लॉक के लिए एक कठिन कार्य-का-प्रमाण खोजने पर काम करती है।
d. जब कोई ग्रंथि कार्य-का-प्रमाण देखता है, तो यह ब्लॉक को सभी ग्रंथियों में प्रसारित करता है।
e. ग्रंथिया ब्लॉक को केवल तभी स्वीकार करती हैं यदि इसमें सभी लेनदेन वैध हैं और पहले से ही खर्च नहीं किए गए हैं।
f. ग्रंथियां ब्लॉक स्वीकृति कि अभिव्यक्ति श्रृंखला में अगले ब्लॉक के निर्माण को स्वीकृत ब्लॉक की हैश को पूर्व हैश मानकर करती है।

ग्रंथियां हमेशा सबसे लम्बी श्रृंखला को ही ठीक मानती हैं और उसे विस्तारित करने के लिए काम करती रहेंगी। यदि दो ग्रंथियां अगले ब्लॉक के अलग-अलग संस्करणों को एक साथ प्रसारित करती हैं, तो कुछ ग्रंथियां पहला या दूसरा ब्लॉक पहले प्राप्त करेंगी। उस स्थिति में, वे जो पहले प्राप्त हुआ उसपर काम करेंगे लेकिन दूसरी शाखा को बचा कर रखेंगे अगर वह सबसे लम्बी हो जाए तो। गुत्थी तब सुलझेगी जब नया कार्य-का-प्रमाण मिलेगा और एक शाखा और लम्बी हो जाएगी, जो ग्रंथियां दूसरी शाखाओं पर काम कर रहे हैं वो भी उन्हें छोड़कर लम्बी शाखा पर आ जाएंगी।

नए लेनदेन के प्रसारण के लिए सभी ग्रंथियों तक पहुंचने की आवश्यकता नहीं है। जब तक वे अनेक ग्रंथियों तक पहुँचते हैं, उस से पहले ही वो एक ब्लॉक में पहुँच जाएंगे। ब्लॉक प्रसारण भी गिराए गए संदेशों के प्रति सहनशील हैं। यदि एक ग्रंथि को एक ब्लॉक प्राप्त नहीं होता है, तो वह उसका अनुरोध तब करेगी जब उससे अगला ब्लॉक मिलने पर उसे एक ब्लॉक की कमी अनुभव होगी।

६. प्रोत्साहन

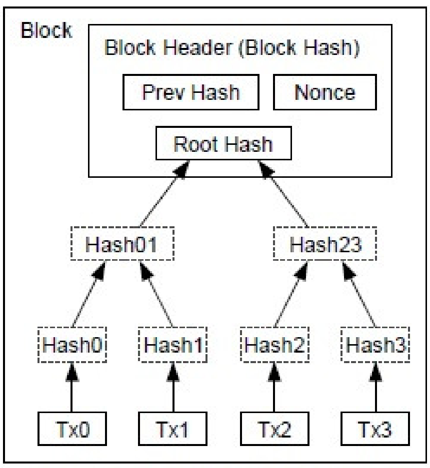
परंपरानुसार ब्लॉक का पहला लेनदेन एक विशेष लेनदेन है जो ब्लॉक के निर्माता के स्वामित्व वाला एक नया सिक्का शुरू करता है। यह ग्रंथियों को नेटवर्क से जुड़ने के लिए प्रोत्साहित करता है, और शुरू में सिक्कों को प्रचलन में लाने का एक तरीका प्रदान करता है, क्योंकि उन्हें जारी करने के लिए कोई केंद्रीय प्राधिकरण नहीं है। नए सिक्कों की नियमित वृद्धि सोने के खनिकों के अनुरूप है जो मुद्राचलन में और सोना जोड़ने के लिए अपने संसाधन व्यय करते हैं। हमारे मामले में, यह सीपीयू समय और ऊर्जा है जो व्यय किया जाता है।

प्रोत्साहन को लेनदेन शुल्क के साथ भी वित्त पोषित किया जा सकता है। यदि किसी लेन-देन का आउटपुट मूल्य उसके इनपुट मूल्य से कम है, तो उनके बीच का अंतर एक लेनदेन शुल्क है जो लेनदेन वाले ब्लॉक के प्रोत्साहन मूल्य में जोड़ा जाता है। एक बार जब पूर्व निर्धारित सिक्के प्रचलन में आ जाएँगे तब प्रोत्साहन राशि लेनदेन शुल्क रहेगा जो की मुद्रास्फीति मुक्त रहेगी।

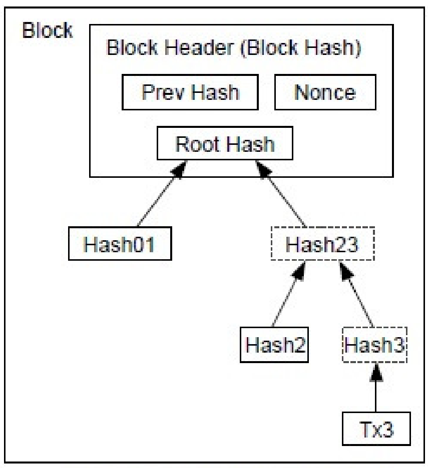
प्रोत्साहन शुल्क ग्रंथियों को ईमानदार रहने के लिए बढ़ावा देगा। अगर एक लालची हमलावर सभी ईमानदार नोड्स की तुलना में अधिक सीपीयू शक्ति को इकट्ठा करने में सक्षम हो जाता है, तो उसे किये गए भुगतान वापिस चुरा कर लोगों को ठगने या फिर उस शक्ति का नए सिक्के उत्पाद करने में से एक निर्णय लेना होगा। उसे नियमों द्वारा खेलना अधिक लाभदायक लगेगा, तंत्र को कमज़ोर और अपने स्वयं के धन की वैधता को कम करने की तुलना में ऐसे नियम जो बाकी सभी से नए सिक्के अर्जित करने में उसका पक्ष लेंगे।

७. डिस्क स्पेस का सुधार

एक बार जब सिक्के का नवीनतम लेनदेन पर्याप्त ब्लॉकों के नीचे दब जाता है, तो इससे पहले के खर्च किये गए सभी लेनदेन को निकाला जा सकता है। इसे बिना ब्लॉक का हैश तोड़े बिना करने के लिए, लेन-देन को एक मर्कल ट्री में हैश किया जाता है [७] [२] [५], केवल रुट को ब्लॉक की हैश में सम्मिलित कर। आंतरिक हैश को संग्रहीत करने की आवश्यकता नहीं है।



Transactions Hashed in a Merkle Tree

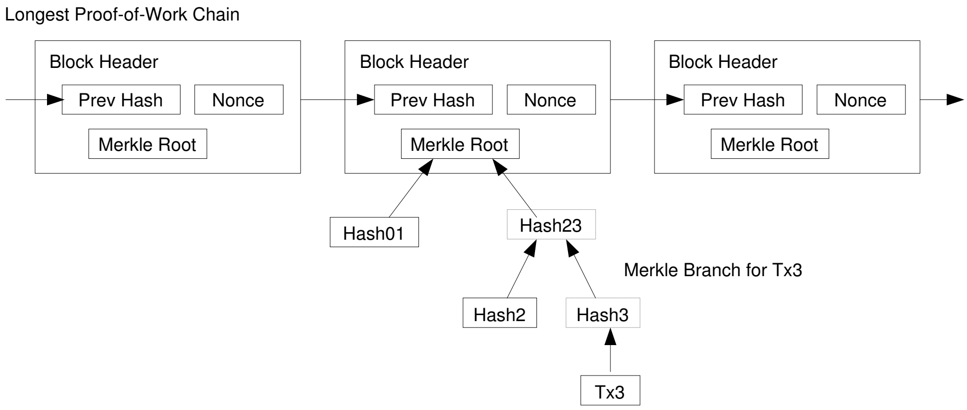


After Pruning Tx0-2 from the Block

बिना लेन-देन वाला ब्लॉक हेडर लगभग 80 बाइट्स का होगा। अगर हम मान लें कि ब्लॉक हर 10 मिनट में उत्पन्न होते हैं, 80 बाइट्स * 6 * 24 * 365 = ४.२ MB प्रति वर्ष। २००८ तक आमतौर पर कंप्यूटर सिस्टम की २GB RAM के साथ बिक्री होती है, और मूर की विधि प्रति वर्ष 1.2GB की वर्तमान वृद्धि की भविष्यवाणी करती है, और ब्लॉक हैडर को स्मृति में रखने पर भी स्टोरेज एक समस्या नहीं होनी चाहिए।

८. सरलीकृत भुगतान सत्यापन

पूर्ण नेटवर्क ग्रंथि चलाए बिना भुगतानों को सत्यापित करना संभव है। एक उपयोगकर्ता को सबसे लम्बी कार्य-का-प्रमाण श्रृंखला के ब्लॉक हेडर की एक प्रति रखने की आवश्यकता होती है, जिसे वह नेटवर्क ग्रंथियों की जांच कर प्राप्त कर सकता है, लेकिन यह जांच जब तक चलेगी जब तक वह आश्वस्त ना हो जाए कि उसके पास सबसे लम्बी श्रृंखला है और लेनदेन को समयछाप किये ब्लॉक से जोड़ने वाली मार्केल शाखा हासिल कर ले। वह खुद के लिए लेनदेन की जांच नहीं कर सकता, लेकिन इसे श्रृंखला में एक जगह जोड़कर वह देख सकता है की नेटवर्क ग्रंथि ने इसे स्वीकार कर लिया है और उसके बाद आगे बढे हुए ब्लॉक भी पुष्टि करते हैं कि नेटवर्क ने इसे स्वीकार कर लिया है।

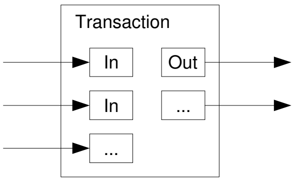


इस प्रकार, सत्यापन तब तक विश्वसनीय है जब तक कि ईमानदार ग्रंथियां नेटवर्क को नियंत्रित करती हैं, लेकिन नेटवर्क को अगर हमलावरों ने काबू कर लिया तो वो ज़्यादा संवेदनशील होगा। जबकि नेटवर्क ग्रंथियां अपने लिए लेनदेन खुद सत्यापित कर सकती हैं, वही सरल विधि को किसी हमलावर के मनगढ़ंत लेनदेन से मूर्ख बनाया जा सकता है जब तक कि हमलावर नेटवर्क को अपने काबू में रख सकता है। इसके बचाव की एक रणनीति, नेटवर्क ग्रंथियों जब एक अमान्य ब्लॉक का पता लगाएं तो उनसे चेतावनी स्वीकार करनी होगी, यह चेतावनी यूज़र के सॉफ्टवेयर को बेजोड़ता की पुष्टि करने हेतु पूरा ब्लॉक और सूचित लेनदेन को डाउनलोड करने के लिए अनुबोधित करेगी। लगातार भुगतान प्राप्त करने वाले व्यवसाय अब भी अधिक स्वतंत्र सुरक्षा और त्वरित सत्यापन के लिए अपनी ग्रंथि चलाना चाहेंगे।

९. संयोजन और विभाजन मूल्य

हालाँकि सिक्कों को व्यक्तिगत रूप से संभालना संभव होगा, लेकिन हस्तांतरण में हर सैंकड़े के लिए एक अलग लेन-देन करना व्यापक होगा। मूल्य को विभाजित और संयुक्त करने की अनुमति देने के लिए, लेनदेन में

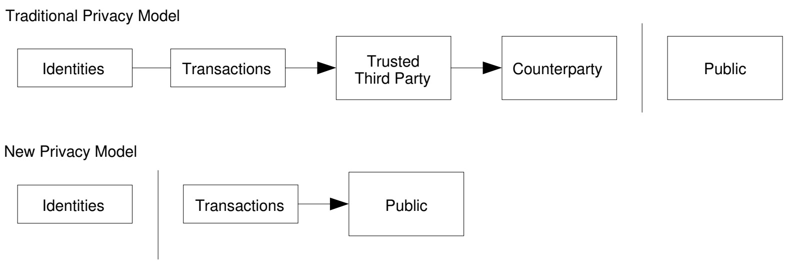
कई इनपुट और आउटपुट होते हैं। आम तौर पर एक बड़े पिछले लेनदेन से या तो एक इनपुट होगा या छोटी मात्राओं के संयोजन वाले कई इनपुट, और अधिकांश दो आउटपुट रहेंगे : एक भुगतान के लिए, और यदि कोई छुट्टा भुगतान हो तो प्रेषक को वापिस देने के लिए।



यह ध्यान दिया जाना चाहिए कि फैन-आउट, जहां एक लेनदेन कई लेनदेन पर निर्भर करता है, और उन लेनदेन पर कई और निर्भर करते हैं, इधर ऐसी कोई समस्या नहीं है। लेन-देन के इतिहास की पूरी स्टैंडअलोन कॉपी निकालने की आवश्यकता कभी नहीं होती है।

१०. गोपनीयता

पारम्परिक बैंकिंग मॉडल शामिल पार्टियों और विश्वसनीय तीसरी पार्टी को सूचना की पहुँच से सीमित करके गोपनीयता के स्तर को हासिल करता है। सभी लेनदेन को सार्वजनिक करने की आवश्यकता इस तरीके को रोकती है, लेकिन गोपनीयता को अभी भी दूसरी जगह सूचना के प्रवाह को तोड़कर बनाए रखा जा सकता है: सार्वजनिक कुंजियों को गुमनाम रखकर। जनता यह देख सकती है कि कोई व्यक्ति किसी और को राशि भेज रहा है, लेकिन बिना लेनदेन की श्रृंखला की सूचना के। यह स्टॉक एक्सचेंजों द्वारा जारी की गई सूचना के स्तर के समान है, जहां व्यक्तिगत ट्रेडों के समय और आकार की "टेप" को सार्वजनिक किया जाता है, लेकिन यह बताए बिना कि कौनसी पार्टी ने क्या लेनदेन किया।



अतिरिक्त फ़ायरवॉल के रूप में, प्रत्येक लेनदेन का एक सार्वजनिक मालिक से जुड़ाव रोकने के लिए हमेशा नयी कुंजी के जोड़ो का इस्तेमाल होना चाहिए। मल्टी-इनपुट लेनदेन के साथ कुछ लिंकिंग अभी भी अपरिहार्य है, जो आवश्यक रूप से प्रकट करते हैं कि उनके इनपुट एक ही मालिक के स्वामित्व में थे । विपत्ति यह है कि यदि एक कुंजी के मालिक का पता चलता है, तो लिंकिंग की प्रक्रिया अन्य लेनदेन जो एक ही मालिक के थे उन्हें भी उजागर कर सकता है।

११. गणना

हम एक हमलावर के परिदृश्य पर विचार करते हैं जो ईमानदार श्रृंखला की तुलना में तेजी से वैकल्पिक श्रृंखला उत्पन्न

करने की कोशिश कर रहा है। यहां तक कि अगर यह पूरा भी किया जाता है, तो यह तंत्र को मनमाने ढंग से बदलाव के लिए नहीं खोलता है, जैसे कि पतली हवा में से मूल्य पैदा करना या ऐसा पैसा लेना जो कभी हमलावर का था ही नहीं। भुगतान के रूप में एक अमान्य लेनदेन को ग्रंथियां स्वीकार नहीं करेंगी, और ईमानदार ग्रंथियां उस ब्लॉक को कभी भी स्वीकार नहीं करेंगे। एक हमलावर केवल अपने स्वयं के लेन-देन में से एक को बदलने की कोशिश कर सकता है ताकि वह हाल ही में खर्च किए गए धन को वापस ले सके।

ईमानदार श्रृंखला और हमलावर श्रृंखला के बीच की दौड़ को एक द्विपद रैंडम वॉक के रूप में चित्रित किया जा सकता है। एक ब्लॉक द्वारा विस्तारित की जाने वाली ईमानदार श्रृंखला सफल परिणाम है, इसकी अग्रणीता को +१ से बढ़ाता है, और विफल परिणाम हमलावर की श्रृंखला का एक ब्लॉक द्वारा विस्तार होना है, जिससे अंतराल -१ से कम हो जाता है।

एक हमलावर को एक दिए गए घाटे से पकड़ने की संभावना एक गैम्बलर रुइन प्रॉब्लम के अनुरूप है। मान लीजिए कि असीमित क्रेडिट से लदा एक जुआरी घाटे में शुरू होता है और ब्रेक - ईवन तक पहुंचने की कोशिश में संभावित रूप से अनंत आज़माइश खेलता है। क्या वह कभी भी ब्रेक-इवन तक पहुंचता है, या कि एक हमलावर कभी भी ईमानदार श्रृंखला के पास पहुँच सकता है, हम उस संभावना की गणना कर सकते हैं जो कि इस प्रकार है [८]:

p = एक ईमानदार ग्रंथि की अगले ब्लॉक को ढूंढ़ने की संभावना

q = हमलावर के अगले ब्लॉक ढूंढ़ने की संभावना

q_z = z ब्लॉक पिछड़े हमलावर आगे वाले ब्लॉक के सामान आने की संभावना

$$q_z = \begin{Bmatrix} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{Bmatrix}$$

हम मान लेते हैं कि p>q है, हमलावर के हमला करने की संभावना तेज़ी से कम होती है क्यूंकि उसे अब ज़्यादा ब्लॉक पार करने होंगे। उसके खिलाफ चल रही बाधाओं के साथ, यदि वह जल्दी से एक झपट्टा नहीं मारता, तो उसके अवसर ना बराबर हो जाते है क्योंकि वह और पीछे हो जाता है।

अब हम विचार करते हैं कि एक नए लेनदेन के प्राप्तकर्ता को कितनी देर तक प्रतीक्षा करने की आवश्यकता है जब तक कि प्रेषक लेनदेन को बदल नहीं सकता। हम मानते हैं कि प्रेषक एक हमलावर है जो प्राप्तकर्ता को यह विश्वास दिलाना चाहता है कि उसने उसे कुछ समय के लिए भुगतान किया है, और कुछ समय पश्चात भुगतान वापिस अपने आप को पलट ले। ऐसा होने पर भुगतान पाने वाला सतर्क हो जाएगा, लेकिन भुगतान करने वाले को उम्मीद है कि तब तक बहुत देर हो जाएगी।

प्राप्ता एक नई कुंजी की जोड़ी उत्पन्न करता है और हस्ताक्षर करने से कुछ समय पहले प्रेषक को सार्वजनिक कुंजी देता है। यह भुगतान करने वाले को, निरंतर उसपर काम करके जब तक की वह भाग्यशाली नहीं होता समय से पहले आगे जाकर एक ब्लॉक की श्रृंखला बनाकर और उसी समय लेनदेन का निष्पादन करने से रोकता है। एक बार लेनदेन भेजे जाने के बाद, बेईमान प्रेषक अपने लेनदेन के वैकल्पिक संस्करण वाले समानांतर श्रृंखला पर गुप्त रूप से काम करना शुरू कर देता है।

भुगतान पाने वाला तब तक प्रतीक्षा करता है जब तक कि लेन-देन को एक ब्लॉक में नहीं जोड़ा जाता है और उस ब्लॉक के बाद 'z' संख्या जितने ब्लॉक जोड़ दिए जाते हैं। उसे पता नहीं है कि हमलावर ने कितनी

प्रगति की है, लेकिन यह मानकर कि ईमानदार ब्लॉक ने प्रति ब्लॉक औसतन अपेक्षित समय लिया है, हमलावर की संभावित प्रगति अपेक्षित मान के साथ पॉइसन वितरण होगी:

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

हमलावर अभी भी पकड़ सकता है या नहीं इसकी संभावना का अनुमान लगाने के लिए, पोइसन घनत्व को हम प्रत्येक प्रगति के मान (पिछड़े बिंदु से आगे बढ़ने की प्रगति की संभावना का मान) से गुणा करते हैं:

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

वितरण की अनंत अनुगामी समूह को जमा करने से बचने के लिए...

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

C कोड में बदलते हुए...

```
#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;
}
```

कुछ प्रतिफल को चलाकर, हम देख सकते हैं कि संभावना z के साथ घातीय रूप से गिर जाती है।

```
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
```

P के लिए हल 0.1% से कम...

```
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
```

१२. निष्कर्ष

हमने भरोसे पर आश्रय किए बिना इलेक्ट्रॉनिक लेनदेन के लिए एक तंत्र प्रस्तावित किया है। हमने डिजिटल हस्ताक्षरों से बने सिक्कों की सामान्य रूपरेखा के साथ शुरुआत की, जो स्वामित्व का मजबूत नियंत्रण प्रदान करता है, लेकिन दोहरे खर्च को रोकने के तरीके के बिना यह तंत्र अधूरा है। इसका हल करने के लिए, हमने कार्य-का-प्रमाण का उपयोग करके सार्वजनिक लेनदेन को रिकॉर्ड कर एक सहकर्मी-से-सहकर्मी नेटवर्क को प्रस्तावित किया, यह सार्वजनिक लेनदेन हमलावर द्वारा बदलाव के लिए जल्दी से कम्प्यूटेशनल रूप से अव्यावहारिक हो जाता है अगर ईमानदार ग्रंथियां सीपीयू शक्ति के बहुमत को नियंत्रित करती हैं। नेटवर्क अपनी असंरचित सादगी में मजबूत है। थोड़े से समन्वय के साथ सभी ग्रंथियां एक ही बार में काम करती हैं। उन्हें पहचानने की आवश्यकता नहीं है, क्योंकि संदेशों को किसी विशेष स्थान पर नहीं भेजा जाता, केवल सर्वोत्तम प्रयास के आधार पर वितरित करने की आवश्यकता होती है। ग्रंथियां नेटवर्क अपनी मर्ज़ी से छोड़ सकती हैं, और उनकी अनुपस्थिति में क्या हुआ इसका सबूत सबसे लम्बी काम-का-प्रमाण आधारित शृंखला को स्वीकार कर फिर से शामिल हो सकती है। वे अपनी सीपीयू ऊर्जा के साथ वोट करते हैं, वैध ब्लॉकों की स्वीकृति प्रदान करते हैं और उन्हें काम करने से इनकार करके अमान्य ब्लॉकों को अस्वीकार करते हैं। इस आम सहमति तंत्र के साथ किसी भी आवश्यक नियम और प्रोत्साहन को लागू किया जा सकता है।

संदर्भ

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

२ 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.

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

४ 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.

५ 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.

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

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

८ W. Feller, "An introduction to probability theory and its applications," 1957.