बिटकॉइन: एक पीअर-टू-पीअर इलेक्ट्रॉनिक कॅश सिस्टम

संतोषी नाकामोटा
satoshin@gmx.com
www.bitcoin.org

अमूर्त. इलेक्ट्रॉनिक कॅशचे एक पूर्णपणे पीअर-टू-पीअर म्हणजेच थेट फक्त दोन व्यक्तींमधील व्यवहार असे स्वरूप... यात कोणत्याही वित्त संस्थेच्या माध्यमातून न जाता ऑनलाइन पेमेंट थेट एका व्यक्तीकडून दुसऱ्या व्यक्तीला पाठवता येते. डिजिटल सिग्नेचरमध्ये या पर्यायाचा काही भाग शक्य होतो. मात्र, विश्वासार्ह तृतीय पक्षाला पैसे चुकून दोनदा पाठवले जाणे टाळण्यासाठी काही उपाय करावे लागणार असतील तर या पद्धतीतील मूळ फायदा मिळतच नाही. आम्ही पीअर-टू-पीअर म्हणजेच थेट दोन व्यक्तींमधील नेटवर्क वापरून डबल स्पेडिंग किंवा पैसे चुकून दोनदा पाठवले जाण्यावर पर्याय पुरवतो. या नेटवर्कमध्ये हॅश-बेस्ड प्रूफ-ऑफ-वर्कच्या चालू साखळीत हे नेटवर्क व्यवहारांना हॅशिंग करून टाइमस्टॅम्प करते. यामुळे व्यवहारांची जी नोंद होते ती प्रूफ-ऑफ-वर्क पुन्हा नव्याने केल्याशिवाय बदलता येत नाही. व्यवहारांची ही भलीमोठी साखळी म्हणजे घडलेल्या घडामोडींचा पुरावा असतेच. शिवाय, सर्वात मोठ्या सीपीयू पॉवरमधून हे शक्य झाल्याचाही तो पुरावा असतो. जोवर नेटवर्कवर हल्ला करण्यासाठी एकमेकांसोबत येऊ न शकणाऱ्या नोड्सतर्फे जोवर बहूतांश सीपीयू पॉवरचे नियंत्रण होत आहे तोवर बाहेरील हल्लेखोरांना दूर ठेवत या प्रणालीत सर्वात मोठी व्यवहार साखळी तयार होत राहील. मुळात, या नेटवर्कला फारच अल्प प्रमाणात आराखडा गरजेचा आहे. सर्वोत्कृष्ट पर्यायांच्या आधारे यात मेसेजेस ब्रॉडकास्ट केले जातात. यात नोड्स हवेतेव्हा नेटवर्कमधून बाहेर पडू शकतात आणि पुन्हा नेटवर्कमध्ये येऊ शकतात. नेटवर्कच्या बाहेर असताना जे काही घडेल त्यासाठी हे नोड्स सर्वात मोठ्या प्रूफ-ऑफ-वर्कला पुरावा म्हणून ग्राह्य धरतात.

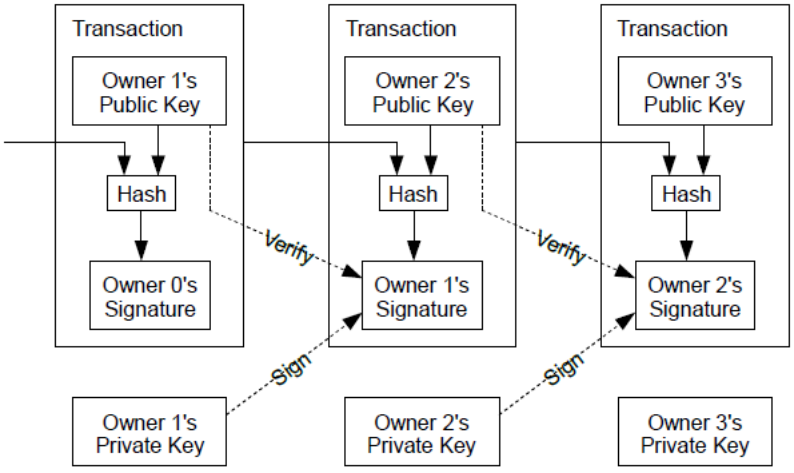
1. ओळख

इंटनेटवरील कॉमर्स किंवा व्यवहार इलेक्ट्रॉनिक पेमेंट पार पाडण्यासाठी पूर्णपणे तृतीय पक्ष म्हणून सेवा देणाऱ्या वित्त संस्थांवर अवलंबून आहेत. बहूतांश व्यवहारांसाठी ही प्रणाली बऱ्यापैकी चांगले काम करत असली तरी त्यात विश्वासावर अवलंबून प्रणालीतील मूळ समस्या किंवा कमतरता असतातच. कोणत्याही प्रकारे मागे घेता येणार नाहीत अशा प्रकारचे व्यवहार खरेतर शक्य नाहीत. कारण यासंदर्भातील विवाद अथवा तक्रारींमध्ये मध्यस्थी करणे या वित्त संस्थांना टाळता येणार नाही. या मध्यस्थीच्या दरामुळे व्यवहारांचा दरही वाढतो. त्यामुळे व्यवहारांवर किमान रकमेची मर्यादा घालावी लागते आणि परिणामी छोट्या साध्यासुध्या व्यवहारांची शक्यता कमी कमी होत जाते. त्यामुळे, मागे न घेता येणाऱ्या सेवांसाठी मागे न घेता येणारे पेमेंट करण्यासाठी ही क्षमता गमावण्याची किंमतही अधिक आहे. रिव्हर्सल म्हणजेच व्यवहार मागे घेण्याची शक्यता म्हणजे अधिक प्रमाणात विश्वासाची गरज आहे. ग्राहकांना त्यांच्या गरजेपेक्षा अधिक माहिती देताना व्यापाऱ्यांनी त्यांच्या ग्राहकांच्या बाबतीत सावध असायला हवे. काही प्रमाणात घोटाळा किंवा फसवणूक होणे हे टाळता न येण्यासारखे आहे, हे आपण मान्य केले आहे. चलनाचा प्रत्यक्ष वापर करून हा खर्च आणि पेमेंटमधील अनिश्चितता प्रत्यक्ष व्यवहारांमध्ये टाळता येऊ शकते. मात्र विश्वासार्ह पक्षाला वगळून इतर कोणत्याही माध्यमातून पेमेंट करता येईल अशी प्रणाली अस्तित्वात नाही.

अशा परिस्थितीत आपल्याला गरज आहे अशा इलेक्ट्रॉनिक पेमेंट सिस्टमची जी विश्वासावर नाही तर क्रिप्टोग्राफिक पुराव्यांवर अवलंबून असेल. ज्यामुळे एकमेकांशी व्यवहार करू इच्छिणाऱ्या कोणत्याही दोन पक्षांना विश्वासार्ह तृतीय पक्षाची गरज न भासता थेट व्यवहार करता येईल. केलेला व्यवहार मागे घेणे संगणकीयदृष्ट्या अव्यवहार्य किंवा अशक्य झाल्यास विक्रेत्याला फसवणुकीपासून संरक्षण मिळेल आणि त्याचसोबत ग्राहकांना संरक्षण देण्यासाठी नियमित एस्क्रो प्रणाली सहज अमलात आणली जाऊ शकते. या लेखातून आम्ही असा पर्याय समोर ठेवत आहोत ज्यात पीअर-टू-पीअर वितरण टाईमस्टॅम्प सर्व्हर वापरून व्यवहारांच्या कालक्रमानुसार पुरावा मांडून करून डबल स्पेंडिंग किंवा चुकून दोनदा पेमेंट होण्याच्या समस्येवर उपाय शोधण्यात आला आहे. कोणत्याही हल्लेखोर नॉड्सच्या एकत्रित गटाहून अधिक ताकदीने प्रामाणिक नोड्स एकत्रितरित्या अधिक सीपीयू तायद नियंत्रित करतील तोवर ही प्रणाली सुरक्षित असेल.

2. व्यवहार

आम्ही इलेक्ट्रॉनिक कॉइनला डिजिटल स्वाक्षऱ्यांची साखळी मानतो. प्रत्येक वापरकर्ता पुढच्या व्यक्तीला कॉइन ट्रान्सफर करण्यासाठी आधीच्या व्यवहाराच्या हॅशवर आणि पुढील मालकाच्या पब्लिक कीवर डिजिटल स्वाक्षरी करतो आणि ते कॉइनच्या शेवटी जोडले जाते. पेमेंट करणारी व्यक्ती चेन ऑफ ओनरशीप किंवा मालकीची साखळी सत्यापित करण्यासाठी स्वाक्षरी सत्यापित करू शकतो.

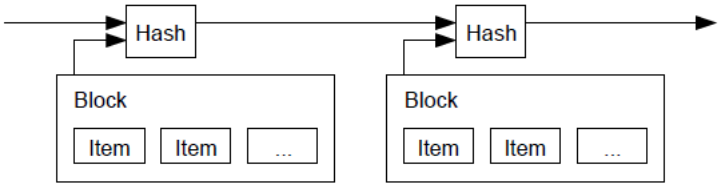


यात प्रश्न असा आहे की मालकाने कॉइन डबल स्पेंड केलेले नाही हे पेमेंट करणाऱ्याला तपासता येत नाही. यासाठी एक सर्वांच्या सोयीचा उपाय म्हणजे एक विश्वासार्ह केंद्रीय अधिकार असलेली प्रणाली किंवा मिंट (टाकसाळ) सादर करणे जिथे डबल स्पेंडिंगच्या दृष्टीने प्रत्येक व्यवहार तपासला जाईल. प्रत्येक व्यवहारानंतर नवे कॉइन जारी करण्यासाठी हे कॉइन मिंटकडे परत जाईल आणि फक्त मिंटकडून थेट जारी झालेले कॉइन्स डबल स्पेंड होणार नाहीत यासाठी विश्वासार्ह ठरतील. या पर्यायातील समस्या अशी आहे की यातील संपूर्ण चलन प्रणाली हे मिंट किंवा टाकसाळ चालवणाऱ्या कंपनीवर अवलंबून असेल. यात बँकेप्रमाणे प्रत्येक व्यवहार या कंपनीच्या माध्यमातूनच होईल.

आधीच्या मालकाने कोणत्याही व्यवहारावर स्वाक्षरी केलेली नाही हे पेमेंट करणाऱ्या व्यक्तीला कळू शकेल असा मार्ग आपल्याला हवा आहे. आपला उद्देश हा आहे की फक्त आधीचा एक व्यवहार ग्राह्य धरला जातो. त्यामुळे त्यानंतरच्या व्यवहारात डबल स्पेंडिंग झाले असले तरी आपल्याला फरक पडत नाही. एखादा व्यवहार गाळला गेला आहे किंवा नाही हे स्पष्ट होण्याचा एकमेव मार्ग म्हणजे सर्व व्यवहारांची माहिती असणे. टाकसाळीवर आधारित प्रणालीमध्ये टाकसाळीला सर्व व्यवहारांची माहिती असते आणि कोणता व्यवहार आधी झाला हे ठाऊक असते. विश्वासार्ह पक्षाविना हा व्यवहार पूर्ण करायचा असेल तर व्यवहार सार्वजनिक स्तरावर जाहीर व्हायला हवा [1] आणि सहभागींना व्यवहार ज्या क्रमाने मिळालेत त्याच्या एका नोंदीवर सर्व सहभागी मंजुरी दर्शवतील अशी प्रणाली आपल्याला हवी आहे. पेमेंट करणाऱ्या व्यक्तीला प्रत्येक व्यवहाराच्या वेळी हा पुरावा हवा असतो की हा व्यवहार प्रथम आहे यावर बहूतांश नोड्स सहमत आहेत.

3. टाईमस्पॅम्प सर्व्हर

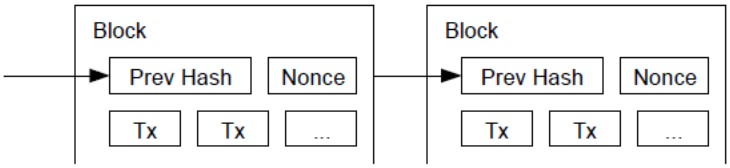
आम्ही जो पर्याय देऊ करत आहोत त्याची सुरुवात होते टाईमस्टॅम्प सर्व्हरपासून. टाईमस्टॅम्प करणाऱ्या वस्तूंच्या गठ्ठ्याचा हॅश घेऊन आणि वर्तमानपत्रे किंवा यूझनेट पोस्टवर मोठ्या प्रमाणावर हॅश प्रसिद्ध करून टाइमस्टॅम्प सर्व्हर काम करते[2-5]. टाईमस्टॅम्पमुळे हे सिद्ध होते की त्या-त्या वेळी संबंधित डेटा अस्तित्वात होता, अर्थातच, हॅशमध्ये समावेश होण्यासाठी अस्तित्वात होता. प्रत्येक टाईमस्टॅम्पमध्ये त्याच्या हॅशमधील आधीचे टाईमस्टॅम्प समाविष्ट असतात. आपल्या आधीच्या टाईमस्टॅम्पचा समावेश करत पुढचा टाईमस्टॅम्प तयार होतो आणि त्यांची एक साखळी बनते.



4. प्रूफ-ऑफ-वर्क

पीअर-टू-पीअर पद्धतीने वितरित टाईमस्टॅम्प सर्व्हर अमलात आणण्यासाठी आपल्याला वर्तमानपत्रे किंवा यूझनेट पोस्टएवजी ॲडम बॅकच्या हॅशकॅशच्या धर्तीवर प्रूफ-ऑफ-वर्क प्रणालीचा वापर करण्याची गरज आहे [6]. प्रूफ-ऑफ-वर्क प्रणालीमध्ये हॅश करताना SHA-256 अशा प्रकारे मूल्याचे स्कॅनिंग केले जाते आणि त्यामुळे शून्य बिट्स संख्येवरून हॅश सुरू होतो. आवश्यक शूनय बिट्सच्या घातांकिय संख्येत सरासरी कार्य आवश्यक असते आणि सिंगल हॅश वापरात आणून ते सत्यापित केले जाऊ शकते.

आमच्या टाईमस्टॅम्प नेटवर्कसाठी , ब्लॉकच्या हॅशला आवश्यक शून्य बिट्स देणारे मूल्य मिळेपर्यंत आम्ही ब्लॉकमध्ये नॉन्स किंवा शून्य संख्या वाढवत प्रूफ-ऑफ-वर्क वाढवत राहतो. एकदा प्रूफ-ऑफ-वर्कसाठी सुयोग्य स्थिती येईपर्यंत सीपीयूचे प्रयत्न यशस्वी झाले की पुन्हा सगळे काम नव्याने केल्याशिवाय ब्लॉकमध्ये बदल करता येत नाही. त्यानंतरचे ब्लॉक साखळीत जोडले जात असल्याने ब्लॉक बदलायचे झाल्यास त्यानंतरच्या सर्व ब्लॉकचे काम नव्याने करावे लागते.



प्रूफ-ऑफ-वर्कमुळे बहूतांश निर्णय प्रक्रियेत प्रतिनिधीत्व निर्धारित करण्याची समस्याही सुटते. यातील बहूतांश बाबी वन-आयपी-ॲड्रेस-वन-वोट तत्वावर आधारित असल्यास कोणीही त्यात अनेक आयपी वितरित करू शकणारे कोणीही यात हस्तक्षेप करू शकेल. प्रूफ-ऑफ-वर्क हे कायमच वन-सीपीयू-वन-वोट असते. यातील बहूतांश निर्णय सर्वात मोठ्या साखळीने दर्शवले जातात. ज्यात प्रचंड प्रमाणावर प्रूफ-ऑफ-वर्क कार्याचा समावेश असतो. बहूतांश सीपीयू पॉवर प्रामाणिक नोड्सने नियंत्रित केले जात असतील तर प्रामाणिक साखळी वेगाने वाढेल आणि स्पर्धात्मक साखळ्यांना मागे टाकेल. त्यामुळे एखाद्या आधीच्या ब्लॉकमध्ये बदल करण्यासाठी हल्लेखोरांना संबंधित ब्लॉकच्या प्रूफ-ऑफ-वर्कमध्ये आणि त्याच्या नंतरच्या सर्व ब्लॉक्समध्ये बदल करावे लागतील. शिवाय, पुन्हा वेगाने वाढणाऱ्या संबंधित ब्लॉकवर परत येऊन प्रामाणिक नोड्सच्या कामांच्या वेगाहून अधिक वेगाने काम करावे लागेल. पुढील ब्लॉक्स वेगाने जोडले जात असताना कमी वेगाने काम करणाऱ्या हल्लेखोरांकडून ब्लॉक उद्ध्वस्त करण्याचा वेग कसा कमी होतो, हे आपण पुढे पाहणारच आहोत. हार्डवेअरचा वाढता वेग आणि नोड्स चालवण्यातील स्वारस्य काळाप्रमाणे बदलणे याची भरपाई करण्यासाठी दर तासाच्या सरासरी ब्लॉक्सला बदलत्या सरासरीने लक्ष्यित करून प्रूफ-ऑफ-वर्कमधील समस्या शोधली जाते. ही निर्मिती वेगाने होत असेल तर समस्या वाढतात.

5. नेटवर्क

नेटवर्क चालवण्यासाठीच्या पायऱ्या खालीलप्रमाणे आहेत:

1) सर्व नोड्सवर नवा व्यवहार ब्रॉडकास्ट केला जातो.
2) प्रत्येक नोड ब्लॉकमध्ये नव्या व्यवहाराला सामावून घेतो.
3) प्रत्येक नोड आपल्या ब्लॉकसाठी कठीण प्रूफ-ऑफ-वर्क शोधण्यासाठी कार्यरत होते.
4) प्रूफ-ऑफ-वर्क सापडल्यानंतर नोड इतर सर्व नोड्सना तो ब्लॉक ब्रॉडकास्ट करतो.
5) ब्लॉकमधील सर्व व्यवहार वैध असतील आणि त्यावर आधीच खर्च झाला नसेल तरच नोड्स संबंधित ब्लॉकचा स्वीकार करतात.
6) साखळीतील पुढील ब्लॉक निर्माण करण्याचे काम सुरू करून नोड आपण संबंधित ब्लॉक स्वीकारल्याचे दर्शवते. यासाठी स्वीकारलेल्या ब्लॉकचा हॅश आधीचा हॅश म्हणून वापरला जातो.

नोड्स नेहमीच सर्वात मोठ्या साखळीला योग्य साखळी म्हणून ग्राह्य धरतात आणि ती अधिक वाढवण्यासाठी कार्यरत राहतात. दोन नोड्सने एकाच वेळी पुढील ब्लॉकच्या वेगळ्या आवृत्त्या ब्रॉडकास्ट केल्या तर काही नॉड्सना त्यातील काही आवृत्त्या आधी प्राप्त होतात. असे झाल्यास, जी आवृत्ती प्रथम प्राप्त झाली त्यावर काम सुरू होते मात्र दुसरी आवृत्ती मोठी असल्यास ती सेव्ह केली जाते. पुढील प्रूफ-ऑफ-वर्क मिळाल्यानंतर ही बरोबरीतील स्पर्धा तोडली जाते आणि एक शाखा मोठी होत जाते. दुसऱ्या शाखेवर काम करणारे नोड्स त्यानंतर मोठ्या साखळीवर काम सुरू करतात.

नव्या व्यवहारांचे ब्रॉडकास्ट सर्व नोड्सकडे पोहोचायलाच हवे, असे आवश्यक नाही. अनेक नॉड्सकडे पोहोचताच क्षणी फारसा विलंब न लावता ते ब्लॉकमध्ये रुपांतरित होतात. ब्लॉक ब्रॉडकास्टमध्ये सुटून गेलेल्या मेसेजसाठीचीही सोय करण्यात आली आहे. नोडला ब्लॉक मिळाला नसेलतर पुढचा ब्लॉक मिळाल्यानंतर मधला एखादा ब्लॉक सुटून गेलाय हे लक्षात येऊन नोड त्यासाठी विनंती पाठवतो.

6. प्रोत्साहन

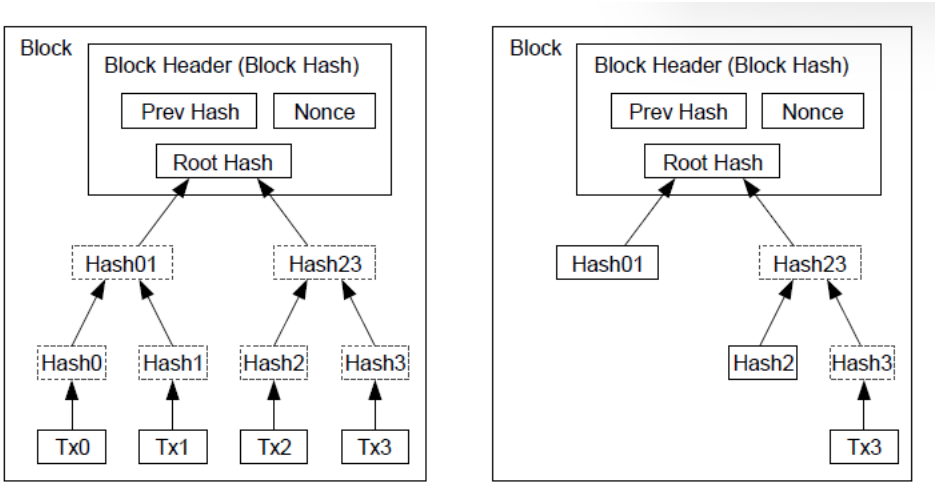
पारंपरिकरित्या, ब्लॉकमधील पहिला व्यवहार हा विशेष व्यवहार समजला जातो. त्यातून ब्लॉकच्या निर्मात्याच्या मालकीच्या नव्या कॉइनची सुरुवात होते. या प्रणालीत कॉइन चलनात आणण्यासाठी कोणत्याही प्रकारची केंद्रीय अधिकृत संस्था नसल्याने यामुळे नोड्सला नेटवर्कला पाठबळ देण्यास प्रोत्साहन मिळते आणि सुरुवातीच्या टप्प्यात कॉइन्स चलनात आणण्याचा मार्ग खुला होतो. ठराविक मूल्याच्या नव्या कॉइन्सची सातत्याने भर पडत राहणे म्हणजे जणू सोने चलनात असावे यासाठी सोन्याच्या खाणीच्या मालकांनी स्रोतांचा सातत्याने विस्तार करणे. या प्रमाणे, आपल्या या परिस्थितीत, सीपीयू वेळ आणि इलेक्ट्रिसिटीचा विस्तार होत असतो.

व्यवहारांवरील शुल्काच्या माध्यमातूनही या प्रोत्साहनांना साह्य केले जाऊ शकते. एखाद्या व्यवहाराचे आऊटपूट मूल्य हे त्याच्या इनपूट मुल्याहून कमी असेल तर त्यातील फरक हा व्यवहार शुल्क असतो आणि तो या व्यवहाराच्या ब्लॉकच्या प्रोत्साहन मुल्यात जोडला जातो. एकदा का ठरलेल्या संख्येइतके कॉइन्स चलनात आले की प्रोत्साहन पूर्णपणे व्यवहार शुल्क म्हणून गणले जाते आणि दर वाढण्यापासून पूर्णपणे मुक्त असते.

प्रोत्साहन शुल्कामुळे नोड्सना प्रामाणिक राहण्याचे प्रोत्साहन मिळते. एखाद्या लोभी हल्लेखोराने प्रामाणिक नोड्सहून अधिक सीपीयू पॉवर मिळवली तर त्याला ती एखाद्या फसव्या माणसाचे पेमेंट पुन्हा चोरण्यासाठी वापरणे किंवा त्या पॉवरमधून नवे कॉइन्स निर्माण करणे अशी निवड करावी लागेल. म्हणजेच त्याला नियमांनुसार खेळणे अधिक फायदेशीर वाटले पाहिजे, असे नियम जे व्यवस्था आणि स्वतःच्या संपत्तीची वैधता कमी करण्यापेक्षा त्याला इतर सर्वांच्या एकत्रित **नाण्यांच्या तुलनेत** अधिक नवीन नाणी देतात.

7. डिस्क स्पेसवर पुन्हा दावा करणे

कॉइनमधील नवा व्यवहार पुरेशा ब्लॉक्सच्या मागे गेला की त्याआधीचे खर्चाचे व्यवहार काढून टाकले जातात आणि डिस्क स्पेस राखली जाते. ब्लॉकचा हॅश न तोडता हे करण्यासाठी व्यवहार मर्कल ट्रीमध्ये [7][2][5] हॅश केले जातात. यात ब्लॉकच्या हॅशमध्ये फक्त मूळ व्यवहाराचा समावेश असतो. या झाडाच्या फांद्या कमी करून जुने ब्लॉक छोट्या स्वरुपात जपले जाते. अंतर्गत हॅश साठवून ठेवण्याची गरज नसते.



Transactions Hashed in a Merkle Tree

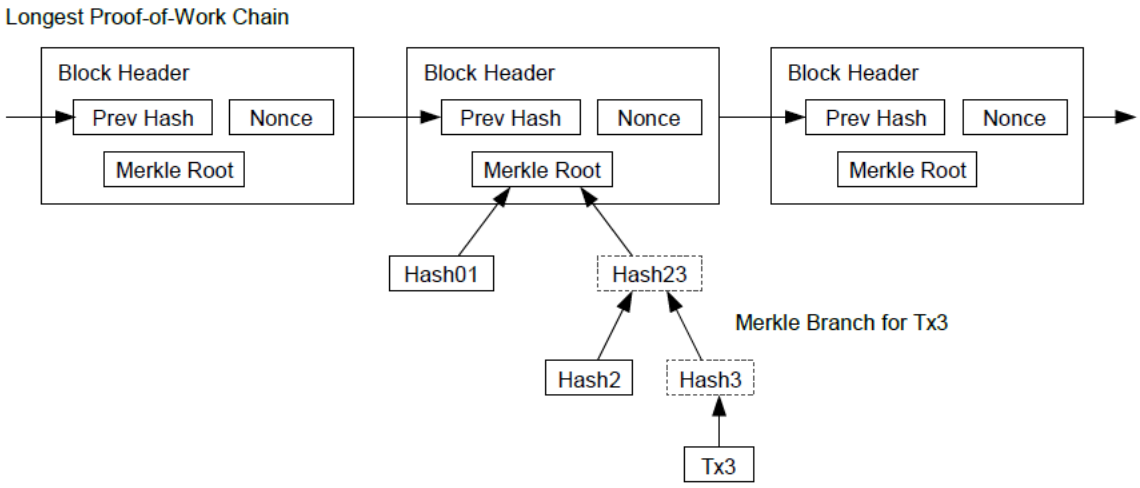
After Pruning Tx0-2 from the Block

कोणताही व्यवहार नसलेला ब्लॉक हेडर साधारण ८० बाइट्सचा असतो. आपण असे गृहित धरू की दर १० मिनिटाला ब्लॉक तयार होतातण् तर वर्षाला 80 bytes *** 6 * 24 * 365 = 4.2**MB**. संगणकीय प्रणाली साधारणपणे २००८ पर्यंत 2**GB of RAM **विकत होते आणि मूरच्या नियमाप्रमाणे सध्याच्या प्रगतीचा अंदाज हा दर वर्षाला १.२ जीबी आहे. असे असल्यास ब्लॉक हेडर्स मेमरीमध्ये ठेवले तरी स्टोरेजची समस्या येणार नाही.**

8. सहजसोपे पेमेंट वेरिफिकेशन

पूर्ण नेटवर्क नोड न चालवता **पेमेंट** सत्यापित करणे शक्य आहे. वापरकर्त्याला फक्त सर्वात लांब प्रुफ-ऑफ-वर्क साखळीच्या ब्लॉक **हेडर्सची** एक प्रत ठेवण्याची आवश्यकता असते, जी त्याला नेटवर्क नोड्सची चौकशी करून त्याच्याकडे सर्वात लांब साखळी असल्याची खात्री होईपर्यंत मिळवता येते आणि ब्लॉक **ज्यात टाईमस्टॅम्प करण्यात आला आहे त्या व्यवहाराची** मर्कल **ब्रांच मिळवता येते.**

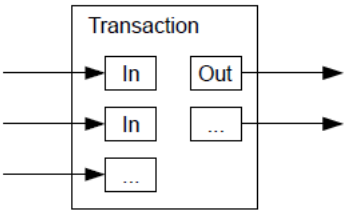
वापरकर्ता स्वतः व्यवहार तपासू शकत नाही, परंतु साखळीतील एका ठिकाणाशी लिंक करून, नेटवर्क नोडने ते स्वीकारले आहे **की नाही हे तो पाडू शकतो** आणि **त्यानंतर** ब्लॉक्स **जोडले गेले असतील तर नेटवर्कने स्वीकारल्याची पुष्टी होते**.



जसे की, प्रामाणिक नोड्स**चे** नेटवर्कवर नियंत्रण **आहे** तोपर्यंत सत्यापन विश्वसनीय असते, परंतु जर नेटवर्क **हल्लेखोराची ताकद अधिक असल्यास ते** असुरक्षित **असण्याची शक्यता वाढते.** नेटवर्क नोड्स स्वतःसाठी व्यवहार सत्यापित करू शकतात, परंतु हल्लेखोर नेटवर्कवर मात **करत असेल तोवर** हल्लेखोराच्या बनावट व्यवहारांद्वारे **या सरळसोप्या पद्धतीला फसवता येऊ शकते.** यापासून संरक्षण करण्यासाठी एक धोरण म्हणजे नेटवर्क नोड्सना अवैध ब्लॉक आढळल्यावर त्यांच्याकडून सूचना स्वीकारणे, वापरकर्त्याच्या सॉफ्टवेअरला पूर्ण ब्लॉक डाउनलोड करण्या**पासून** प्रवृत्त करणे आणि विसंगतीची पुष्टी करण्यासाठी अलर्ट केलेले व्यवहार. ज्या व्यवसायांना वारंवार देयके मिळतात त्यांना अधिक स्वतंत्र सुरक्षितता आणि जलद पडताळणीसाठी त्यांचे स्वतःचे नोड्स चालवायचे असतील.

9. मूल्य एकत्र करणे आणि विभाजित करणे

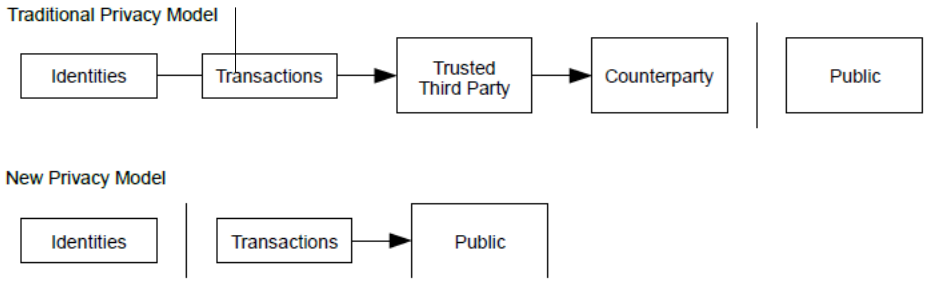
कॉइन्स वैयक्तिकरित्या हाताळणे शक्य असले तरी, हस्तांतरणामध्ये प्रत्येक सेंटसाठी स्वतंत्र व्यवहार करणे अजिबात कठीण नाही. मूल्य विभाजित आणि एकत्रित करण्याची अनुमती देण्यासाठी, व्यवहारांमध्ये एकाधिक इनपुट आणि आउटपुट असतात. **साधारणपणे** पूर्वीच्या मोठ्या व्यवहारातून एकतर एकच इनपुट किंवा लहान रकमेचे एकत्रीकरण करणारे अनेक इनपुट आणि जास्तीत जास्त दोन आउटपुट असतील: एक पेमेंटसाठी, आणि एक बदल, जर असेल तर, **पाठवणाऱ्याला** परत करेल.



हे लक्षात घेतले पाहिजे की फॅन-आउट, जेथे एक व्यवहार अनेक व्यवहारांवर अवलंबून असतो आणि ते व्यवहार अनेकांवर अवलंबून असतात, **ही या ठिकाणी समस्याच नाही.** व्यवहाराच्या **नोंदींची** संपूर्ण स्वतंत्र प्रत काढण्याची कधीही गरज नसते.

10. गोपनीयता

पारंपारिक बँकिंग मॉडेल **संबंधित** पक्षांना आणि विश्वासार्ह तृतीय पक्षां**साठी** माहिती**ची उपलब्धता** मर्यादित **ठेवून** गोपनीयतेची **एक ठराविक** पातळी प्राप्त करते. सर्व व्यवहार सार्वजनिकपणे जाहीर करण्याची गरज या पद्धतीला प्रतिबंधित करते, परंतु तरीही अन्य ठिकाणी माहितीचा प्रवाह खंडित करून गोपनीयता राखली जाऊ शकते**... यासाठी पब्लिक कीज निनावी ठेवता येतात. इथे इतर** लोक **हे** पाहू शकतात की **एक व्यक्ती दुसऱ्या व्यक्तीला** रक्कम पाठवत आहे, परंतु **या व्यवहाराची माहिती कोणाशीही संबंधित नसते**. हे स्टॉक एक्स्चेंजद्वारे जारी केलेल्या माहितीच्या पातळीसारखेच आहे, जेथे वैयक्तिक व्यापारांची वेळ आणि आकार, "टेप" सार्वजनिक केली जाते, परंतु पक्ष**कार** कोण होते हे न सांगता.



अतिरिक्त फायरवॉल **किंवा सुरक्षा उपाय** म्हणून, प्रत्येक व्यवहारासाठी एक नवीन की **पेअर** वापरण्यात यावी**. त्यामुळे ते एकाच मालकाशी जोडले जाणार नाही. मल्टि**-इनपुट व्यवहारांसह काही लिंकिंग अद्याप अपरिहार्य आहे**. त्यामुळे त्या व्यवहारांचे इनपुट एकाच मालकाचे होते हे कळणे** अनिवार्य **होते. इथे** जोखीम अशी आहे की जर एखाद्या कीचा मालक उघड झाला तर, लिंक केल्याने त्याच मालकाचे इतर व्यवहार**ही** उघड होऊ शकतात.

11. गणना

प्रामाणिक साखळीपेक्षा अधिक वेगाने पर्यायी साखळी निर्माण करण्याचा प्रयत्न करणाऱ्या **हल्लेखोरांची** परिस्थिती**ही** आम्ही विचा**रात घेतो. समजा, तसे झालेच तरी, असेच कुठून तरी मूल्य निर्माण करणे किंवा हल्लेखोरांनी इतरांचे पैसे घेणे अशा परिस्थितीसाठी ही प्रणाली कुचकामी ठरत नाही.** नोड्स अवैध व्यवहार पेमेंट म्हणून स्वीकारणार नाहीत आणि प्रामाणिक नोड्स कधीही त्यात असलेला ब्लॉक स्वीकारणार नाहीत. हल्लेखोराने नुकतेच खर्च केलेले पैसे परत घेण्यासाठी फक्त त्याच्या स्वतःच्या व्यवहारांपैकी एक **व्यवहार** बदलण्याचा प्रयत्न करू शकतो.

प्रामाणिक **साखळी** आणि **हल्लेखोरांची साखळी** यांच्यातील शर्य**तीला बायनॉमिनल** रँडम वॉक **म्हणता येईल.** प्रामाणिक शृंखला एका ब्लॉकने वाढवणे, त्याची आघाडी +**1** ने वाढवणे **हे यातील यश आहे** आणि आक्रमणकर्त्याची साखळी एका ब्लॉकने वाढवणे, अंतर -**1** ने कमी **होणे हे यातील अपयश आहे.**

दिलेल्या **तुटी**मधून हल्लेखोर पकडण्याची संभाव्यता जुगाराच्या विध्वंस समस्ये**सारखी** आहे. समजा

अमर्याद क्रेडिट असलेला जुगारी **तुटीपासून सुरुवात करतो आणि** आणि ब्रेकईव्हनपर्यंत पोहोचण्याचा प्रयत्न करण्यासाठी संभाव्यपणे असंख्य चाचण्या खेळतो. तो कधी**तरी** ब्रेकईव्हनपर्यंत पोहोचेल किंवा हल्लेखोर कधी**तरी** प्रामाणिक साखळीला पकडेल या संभाव्यतेची आम्ही खालीलप्रमाणे गणना करू शकतो **[8]:**

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

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

$p > q$ हे आमचे गृहितक लक्षात घेता, ब्लॉक्सची संख्या वाढल्यामुळे **हल्लेखोराला किती ब्लॉक्स गाठावे लागतील याचे प्रमाण वाढते आणि ती शक्यता** झपाट्याने कमी होते. **या शक्यता त्याच्या विरोधात असल्याने** जर त्याने **वेगाने** पुढे नशीबवान झेप घेतली नाही, तर तो आणखी मागे पडल्यामुळे त्याची **जिंकण्याची** शक्यता कमी होते.

पैसे पाठवणारी व्यक्ती व्यवहा**रात बदल करू शकणार नाही** याची पुरेशी खात्री होण्यापूर्वी नवीन व्यवहाराच्या प्राप्तकर्त्याला किती काळ प्रतीक्षा करावी लागेल याचा **आता विचार करूया**. असे गृहीत ध**रूया** की **पैसे पाठवणारी व्यक्ती एक हल्लेखोर आहे जो** प्राप्तकर्त्याला **काही काळ हा** विश्वास **देऊ पाहतोय की** की त्याने त्याला पैसे दिले आहेत. **त्यानंतर** काही वेळ निघून गेल्यानंतर **ते पैसे तो परत स्वत:कडे वळवेल. असे झाल्यास** प्राप्तकर्त्याला सतर्क केले जाईल. **मात्र, पैसे पाठवणाऱ्याला म्हणजेच हल्लेखोराला वाटत राहील की यासाठी फार उशीर झालाय.**

प्राप्तकर्ता एक नवीन की **पेअर** तयार करतो आणि स्वाक्षरी करण्यापूर्वी **पैसे पाठवणाऱ्याला पब्लिक की देतो. त्यामुळे, त्यावर सातत्याने काम करून फाय पुढे जाण्याइतपत नशीबवान ठरेपर्यंत पैसे पाठवणाऱ्याला वेळेआधीच ब्लॉक साखळी तयार करण्यापासून रोखले जाते.** त्यानंतर त्या**च क्षणाला तो** व्यवहार पूर्ण करतो. एकदा व्यवहार पाठवल्यानंतर, अप्रामाणिक **हल्लेखोर** त्याच्या व्यवहाराची पर्यायी आवृत्ती असलेल्या समांतर साखळीवर गुप्तपणे कार्य करण्यास सु**रु**वात करतो.

व्यवहार ब्लॉकमध्ये जोडले जाईपर्यंत आणि z ब्लॉक्स नंतर जोडले जाईपर्यंत प्राप्तकर्ता प्रतीक्षा करतो. हल्लेखोराने नेमकी किती प्रगती केली हे त्याला माहीत नाही, परंतु प्रामाणिक ब्लॉक्सने प्रति ब्लॉक सरासरी अपेक्षित वेळ घेतला असे गृहीत धरल्यास, **हल्लेखोराची** संभाव्य प्रगती अपेक्षित मूल्यासह पॉसॉन वितरण असेल:

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

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

विश्वासावर अवलंबून न राहता इलेक्ट्रॉनिक व्यवहारांसाठी एक प्रणाली **आम्ही सादर करत आहोत.** डिजिटल स्वाक्षरींपासून बनवलेल्या नाण्यांच्या **सर्वसाधारण प्रणालीपासून आम्ही** सुरुवात केली. **यात मालकीहक्कांचे दमदार** नियंत्रण **मिळते. मात्र, डबल स्पेंडिंग टाळण्यासाठीच्या मार्गांशिवाय ही प्रणालीअपूर्ण ठरेल. या समस्येवर तोडगा काढण्यासाठी** आम्ही व्यवहारांचा सार्वजनिक इतिहास रेकॉर्ड करण्यासाठी प्रूफ-ऑफ-वर्क वापरून पीअर-टू-पीअर नेटवर्क प्रस्तावित केले आहे**. प्रा**माणिक नोड्स **बहूतांश सीपीयू** पॉवर नियंत्रित करत असल्यास आक्रमणकर्त्यासाठी **हे नेटवर्क** त्वरीत संगणकीयदृष्ट्या अव्यवहार्य बनतात. **हे** नेटवर्क त्याच्या असंरचित साधेपणामध्ये**ही फार** मजबूत आहे. **सर्व** नोड्स थोड्या**फार** समन्वयाने एकाच वेळी कार्य करतात. **त्यांची ओळख पटवण्याची गरज नसते.** कारण**, हे** संदेश कोणत्याही विशिष्ट ठिकाणी पाठवले जात नाहीत आणि केवळ सर्वोत्तम प्रयत्नांच्या आधारावर वितरित करणे आवश्यक **असते.** नोड्स इच्छेनुसार नेटवर्क सोडू शकतात आणि पुन्हा सामील होऊ

शकतात, ते **नसतानाच्या काळात काय झाले यासाठी** पुरावा म्हणून **प्रूफ-ऑफ-वर्कचा वापर करता येतो.** ते त्यांच्या **सीपीयू पॉवरच्या साहयाने** मत **प्रदर्शित करतात,** वैध ब्लॉक्सचा विस्तार करण्याचे काम करून त्यांची स्वीकृती व्यक्त करतात आणि अवैध ब्लॉक्सवर काम करण्यास नकार देऊन नाकारतात. या सर्वसंमतीच्या यंत्रणेद्वारे कोणतेही आवश्यक नियम आणि प्रोत्साहन लागू केले जाऊ शकतात.

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.