बिटकॉइन वाइट पेपर का हिंदी अनुवाद

(क्रिप्टो न्यूज़ हिंदी द्वारा)

प्रयोजक- "वज़ीरएक्स क्रिप्टो एक्सचेंज"

Created by

Crypto News Hindi
www.cryptonewshindi.com

Sponsored by

WazirX
www.wazirx.com

भूमिका

क्रिप्टो न्यूज़ हिंदी वेबसाइट **www.cryptonewshindi.com** की शुरुआत 26 जनवरी 2019 को की गई थी। इस वेबसाइट को शुरू करने का उद्देश्य भारत में रह रहे क्रिप्टो समुदाय को उनकी भाषा हिंदी में क्रिप्टो की जानकारी और खबरें उपलब्ध करवाना ब्लॉकचेन की जानकारी देना और क्रिप्टो ब्रांड्स को विज्ञापन के लिए सस्ता मंच उपलब्ध करवाना है। क्योंकि विश्व में जितनी भी क्रिप्टो की जानकारी देने वाली वेबसाइट हैं उनमें से अधिकतर अंग्रेजी भाषा में हैं और बहुत बड़ी संख्या में भारतीयों के लिए इस भाषा में बात को समझ पाना मुश्किल होता है, इस लिए क्रिप्टो न्यूज़ हिंदी ने एक प्रयास किया की क्रिप्टो की सभी तरह की जानकारी को आसानी से समझ आने वाली भाषा हिंदी में क्रिप्टो समुदाय तक पंहुचाया जाए। एक साल के अंदर ही क्रिप्टो न्यूज़ हिंदी ने भारतीय क्रिप्टो समुदाय में अपना एक विशेष स्थान बनाया है।

बिटकॉइन वाइट पेपर का हिंदी अनुवाद

बिटकॉइन क्रिप्टो बाजार का जन्म दाता है और बिटकॉइन को अगर समझना है तो इसकी शुरुआत का वह दस्तावेज पढ़ना और समझना जरूरी है जिसमें इसके जनक **सातोशी नाकामोटो** ने बिटकॉइन की हर एक जानकारी को लिखा और वह है **"बिटकॉइन वाइट पेपर"**। हालांकि बिटकॉइन के वाइट पेपर का हिंदी अनुवाद बाजार में उपलब्ध है और आप गूगल के द्वारा भी इसे अपनी भाषा में बदल सकते हैं, लेकिन उसका अनुवाद इतना शुद्ध नही है की एक आम इंसान को समझ मे आ सके,साथ ही यह अनुवाद था विश्लेषण नहीं। क्रिप्टो न्यूज़ हिंदी यहां न केवल बिटकॉइन के वाइट पेपर का हिंदी अनुवाद कर रहा है बल्कि इसका विश्लेषण भी कर रहा है ताकि हर उस लाइन का मतलब समझ आ सके जिसे पढ़ कर बिटकॉइन की गहन जानकारी हो,और बिटकॉइन का पूर्ण ज्ञान मिल सके। हमने कुछ शब्दों के साथ कुछ नंबर लिखें हैं जिनकी व्याख्या इस दस्तावेज के अंत में की गई है , आप वहां से शब्दों के मतलब को गहराई से समझ सकते हैं।इस दस्तावेज में जो गणितीय उदहारण,फार्मूला या इकाइयां दी गई हैं उनसे किसी भी तरह की छेड़छाड़ नहीं की गई हैं बल्कि इसे बिल्कुल वैसे ही लिखा गया है जैसा की असली बिटकॉइन वाइट पेपर में दिया गया है।

क्योंकि बिटकॉइन की जानकारी के बिना क्रिप्टो बाजार को समझना मुश्किल है इस लिए हर एक व्यक्ति तक बिटकॉइन की जानकारी पहुचाने के साथ ही बिना किसी शुल्क के लोगों तक इस वाइट पेपर को पहुँचना हमारा उद्देश्य है। अगर इस अनुवाद में या शब्दों में कोई त्रुटि हो तो हम पहले से ही क्षमा प्रार्थी हैं, हालांकि हमारा यह पूर्ण प्रयास है की यह वाइट पेपर पूरी तरह दोषरहित हो। हम उम्मीद करते हैं की आपको हमारा यह प्रयास पसंद आएगा। हम चाहतें हैं की हर एक प्रोजेक्ट का हिंदी अनुवाद जरूर हो ताकि भारतीय क्रिप्टो समुदाय प्रोजेक्ट की सही जानकारी ले सके।

हमारा यह प्रयास सफल बनाने के लिए हम वज़ीरएक्स एक्सचेंज का दिल से आभार व्यक्त करते हैं जिनके सहयोग से हम दुनिया भर के हिंदी भाषी लोगों तक बिटकॉइन का वाइट पेपर हिंदी में पहुंचाने में सफल हो पाए।हम अपने सभी सहोगियो का भी दिल से धन्यवाद करते है जिन्होंने बिना किसी स्वार्थ के “बिटकॉइन वाइट पेपर” भारतीय क्रिप्टो जगत तक पहुंचाने में हमारी सहायता की । इन सभी के सहयोग के बिना हमारा यह प्रयास सफल न हो पता ।

इस विषय में किसी भी तरह की जानकारी के लिए cryptonewshindi7@gmail.com पर संपर्क किया जा सकता है।

वजीरएक्स के बारे में-वज़ीरएक्स भारत की सबसे सफल क्रिप्टो एक्सचेंज है जिसकी शुरुआत 2018 में की गयी थी,यह बाइनेंस ग्रुप का हिस्सा है जो दुनिया की सबसे बड़ी एक्सचेंज है और 180 देशों में अपनी सेवाएं दे रही है।

2018 में रिज़र्व बैंक की क्रिप्टो लेनदेन के लिए बैंक का इस्तेमाल पर रोक के बाद कई क्रिप्टो एक्सचेंज या तो बंद हो गई या भारत छोड़ गई लेकिन वज़ीरएक्स ने भारतीय क्रिप्टो समुदाय का साथ दिया और विश्व का पहला क्रिप्टो **P2P** विकल्प दिया जहां लोग बिना रुकावट क्रिप्टो का लेनदेन कर सकें।इसी समय वज़ीरएक्स के **संस्थापक निश्चल शेट्टी** ने ट्विटर पर **#INDIAWANTSCRYPTO** अभियान चलाया जो एक जन आंदोलन बन गया,यह अभियान अभी भी जारी है लोगों को शिक्षित करने के लिए और इसे एक साल से ज्यादा का समय हो गया है।वज़ीरएक्स और निश्चल शेटी के सोशल मीडिया की पंहुच 3 मिलियन लोगों तक है।वज़ीरएक्स लगातार प्रगति करता हुआ भारतीय क्रिप्टो ग्रुप है जो बड़े स्तर पर क्रिप्टो की सेवाएं प्रदान कर रहा है।

बीइटकॉइन वाइट पेपर(क्रिप्टो न्यूज़ द्वारा हिंदी में)

बिटकॉइन:एक पियर टू पियर एलेक्ट्रोनिक नकद प्रणाली - सातोशी नाकामोटो

satoshi@gmx.com
www.bitcoin.org

(पियर टू पियर- एक कंप्यूटर प्रणाली है जो एक दूसरे के साथ इंटरनेट से जुडी है बिना किसी केन्द्रीय सर्वर के[1], दूसरे शब्दों में इस प्रणाली के साथ जुड़ा हर एक कंप्यूटर एक सर्वर है जो बिना किसी निजी हस्तक्षेप के फाइल का लेनदेन कर सकता है जिस से यह लेनदेन[2] निजी रहता है।)

सार-एलेक्ट्रोनिक नकद लेनदेन पियर टू पियर प्रणाली के माध्यम से ऑनलाइन एक व्यक्ति से दूसरे व्यक्ति तक भुगतान करने की सुविधा बिना किसी वित्य संस्थान के हस्तक्षेप के उपलब्ध करेगा (जैसे आज हम बैंक,पेटीएम या गूगलपे की मदद लेते हैं पैसा भेजने के लिए,बिटकॉइन एक ऐसी प्रणाली देगा जिसमें दो लोगों के लेनदेन के बीच कोई और नहीं होगा)।

डिजिटल हस्ताक्षर आंशिक समाधान ही देते हैं, लेकिन असल फायदा तब खत्म हो जाता जब दोहरे व्यय को कम करने के लिए तीसरे पक्ष की जरुरत पड़े।हम इस दोहरे व्यय की समस्या को रोकने के लिए पियर टू पियर नेटवर्क को पेश करते हैं।नेटवर्क हैश प्रूफ ऑफ़ वर्क पर आधारित दस्तावेजो की चालू श्रृंखला[3] है जो लेनदेन की प्रविष्टियों[4] को दर्ज करके टाइम्सस्टैम्प[5] करता है जिसे दोबरा किए बिना बदला नहीं जा सकता। (यह एक रजिस्टर की तरह है जिसमें लेनदेन का रिकॉर्ड समय के साथ होगा जिसे बदलना मुश्किल होगा क्योंकि ऐसा करने के लिए सारे रजिस्टर की एन्ट्री को मिटा कर दोबारा लिखना पड़ेगा और चलती हुई ब्लॉकचेन में यह करना संभव नहीं होगा)।सबसे लंबी चेन न केवल हुई घटनाओं को सही क्रम में प्रमाण के रूप में रखेगी बल्कि वह यह भी प्रमाणित करेगी की यह कंप्यूटर CPU की सबसे बड़ी श्रृंखला से आई है।

जब तक अधिकांश CPU शक्ति को ऐसे नोड्स[6] नियंत्रित करते हैं जो नेटवर्क पर हमला करने में सहयोग नहीं देते,तब तक यह सबसे लंबी चेन बनाएंगे और हमलावर[7](अटैकर)को रोकेंगे(नोड्स-वह उपकरण या डाटा संग्राहक हैं जो एक बड़े नेटवर्क के साथ जुड़ कर बड़ी श्रृंखला बनाते हैं जैसे कंप्यूटर,फ़ोन जैसे उपकरण जिनकी मदद से लेनदेन की जानकारी की प्रविष्टियां दर्ज की जाती है)।नेटवर्क के लिए न्यूनतम संरचना की जरुरत होती है।सन्देश श्रेष्ठ प्रयास के आधार पर प्रसारित किए जाते हैं,नोड्स अपने अनुपस्थिति में जो हुआ उसके प्रमाण के रूप में प्रूफ और वर्क की सबसे लंबी चेन और स्वीकार करके इच्छा अनुसार नेटवर्क को छोड़ सकते हैं और फिर उसमें जुड़ सकते हैं।

1. प्रस्तावना
Introduction

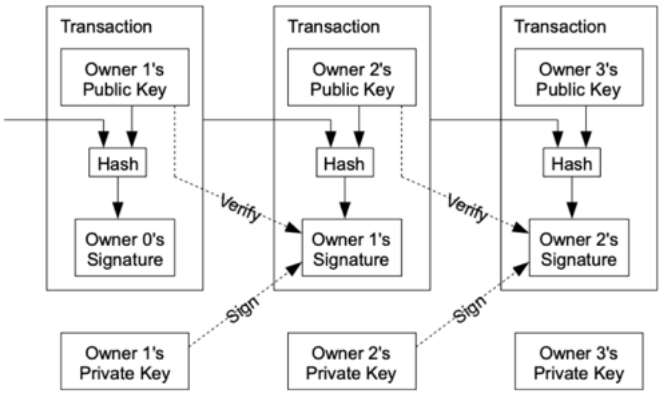
इंटरनेट पर व्यापार के भुगतानों को पूरा करने के लिए आज हम पूरी तरह से तीसरे भरोसेमंद संस्थानों पर निर्भर हैं(अगर हमें किसी खरीद बेच की कीमत देनी है तो बैंक या पेमेंट गेटवे के इस्तेमाल के इलावा हमारे पास कोई विश्वसनीय स्त्रोत नहीं है)।हालांकि यह प्रणाली बहुत अच्छे ढंग से सभी लेनदेन को पूरा करती है,लेकिन इसमें अब भी विश्वास आधारित मॉडल की कुछ आंतरिक कमियां हैं।पूरी तरीके से लेनदेन वापिस न की जा सकने वाली प्रक्रिया नहीं है,वित्य संस्थान समस्या के समय मध्यस्तता करने से नहीं बच सकते। मध्यस्तता की कीमत लेनदेन की कीमत बढ़ा देते हैं,यह कम से कम लेनदेन को खत्म करता है,और वापिस न की जा सकने वाले लेनदेन के लिए व्यापक लागत लगती है।लेनदेन वापसी के लिए भरोसे की जरुरत पड़ती है।

व्यापारियों को अपने ग्राहकों से ज्यादा सावधान रहना पड़ता है और इसके लिए वह ग्रहकों की ज्यादा से ज्यादा जानकारी ले कर उन्हें परेशान करते हैं जिसकी उन्हें जरुरत नहीं होती।इसमें कुछ सीमा तक धोखाधड़ी अनिवार्य मानी जाती है।कैश लेनदेन के द्वारा इस लेनदेन की फीस और धोखे से बचा जा सकता है लेकिन संचार के माध्यम(online transaction)बिना किसी वित्य संस्थान की मदद के बिना नहीं हो सकता। जरुरत है विश्वास के बजाय क्रिप्टोग्राफी प्रमाण पर आधारित भुगतान प्रणाली की जो बिना किसी तीसरे पक्ष की जरुरत के बिना दो पक्षो के लेनदेन को पूरा होने दे।लेनदेन की प्रविष्टियां जिन्हें वापिस करना या निरस्त करना असंभव हो यह विक्रेता को धोखे से बचाएगा और नियमित एस्क्रो प्रणाली को खरीदारों की रक्षा के लिए क्रियान्वित किया जा सकेगा।इस पेपर में हम वह समाधान रख रहे हैं जो दोहरे खर्चे की समस्या को पेअर टू पेअर से समाधान देगा, जो लेनदेन के काल क्रमांक को टाइम स्टेम्प में दर्ज करेगा।यह प्रणाली तब तक सुरक्षित है जब तक ईमानदार[8] नोड्स समूह हमलावर नोड्स के सदस्यों से ज्यादा CPU ताकत को संयुक्त रूप से नियंत्रित करते रहेंगे।

(सार-ऑनलाइन लेनदेन के लिए वित्य संस्थाओं जैसे बैंक और गूगल पे जैसे सिस्टम खत्म करना क्योंकि इन्हें खरीद से धोखे से बचने के लिए उनकी निजी जानकारी लेनी पड़ती है।वित्य संस्थाएं लेनदेन को निरस्त कर सकती हैं जो सुरक्षिक्त नहीं है और यह खर्चो को बढ़ाता है।पेअर टू पेयर इसका समाधान है जिसमें दर्ज लेनदेन की पूरी जानकारी। होती है और इसे किसी भी तरह से बदला नहीं जा सकता,इसके लिए ईमानदार नोड्स वाले समूह की जरुरत है जो इस नेटवर्क पर हमला करने वाले समूह से ज्यादा CPU ताकत लगातार बनाए रखेंगे)

2. लेनदेन
Transactions

एलेक्ट्रोनिक कॉइन[9](बिटकॉइन) को हम डिजिटल हस्ताक्षर की एक श्रृंखला के रूप में परिभाषित करते हैं। प्रत्येक मालिक पिछले लेनदेन के हैश और अगले मालिक की सार्वजनिक कुंजी(रिसीव करने वाले की पब्लिक की बिटकॉइन एड्रेस)पर डिजिटल हस्ताक्षर करके और उसे कॉइन के अंत में जोड़ कर अगले मालिक को कॉइन भेजता है।भेजने वाला स्वामित्व की चेन को सत्यापित(वेरिफाई)करने के लिए हस्ताक्षरों को सत्यापित कर सकता है।(इस बात को नीचे के चित्र से समझें।

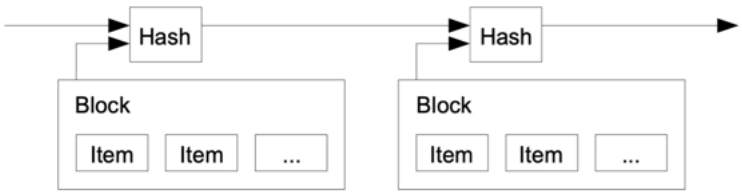


निश्चित तौर पर समस्या यह है की देने वाला यह नहीं जाँच कर सकता की मालिकों में से किसी ने कॉइन को दो बार तो खर्च नहीं कर दिया(डबल ट्रंज़ेक्शन)।इसका एक सामान्य समाधान है की एक विश्वास वाले केंद्रीय प्राधिकारी(वलिडेटर) या टक्साल[10](माइनर)को लाना।हर एक लेनदेन के बाद कॉइन को टक्साल में लौटाया जाना चाहिए,और यही बात का प्रमाण होगा की माईनिंग से आया कॉइन का दोहरा व्यय नहीं हुआ है(मतलब की अगर हमें इस कमी को खत्म करना है की जो बिटकॉइन भेजा जा रहा है उसे दो बार या ज्यादा बार नहीं भेजा गया है तो इसे माईनिंग से निकलना पड़ेगा और माईनिंग से हो कर जो बिटकॉइन पंहुचेगा वह इस बात की गारंटी होगा की इसे दो बार नहीं खर्चा गया है)।इस समाधान की भी एक समस्या है की पूरी धन प्रणाली लेनदेन का परिणाम टक्साल चलाने वाली कंपनी(माईनिंग कंपनी)पर निर्भर करता है,क्योंकि एक बैंक लेनदेन की तरह हर एक लेनदेन को माईनिंग से निकलना पड़ता है।

हम एक ऐसा तरीका चाहते हैं जिसमें कॉइन देने वाला यह जान सके की पिछले मालिकों ने पहले किन्हीं लेनदेन पर हस्ताक्षर नहीं किए थे(जैसे हम कोई जमीन खरीदें तो हमें यह पता होना चाहिए की जो हमें बेच रहा है उसने इस से पहले यही जमीन किसी और को तो नहीं बेची हुई और अगर ऐसा है तो यह धोखा हो जाएगा।इसी समस्या का समाधान यहां निकालने की बात की जा रही है)।हमारे उद्देश्यों के लिए पहले के लेनदेन महत्वपूर्ण हैं, इस लिए हम दोहरे लेनदेन के बाद के परिणामो की परवाह नहीं करते।लेनदेन की अनुपस्तिथि की पुष्टि करने का एक ही तरीका है की सभी लेनदेन के बारे में पता हो(record of every transaction)।टकसाल आधारित मॉडल में टकसाल को सभी लेनदेन की जानकारी रहती है और इस बात का निर्णय करती है की कौन सा लेनदेन पहले प्राप्त हुआ है।

3. टाइमस्टैम्प सर्वर
Timestamp Server

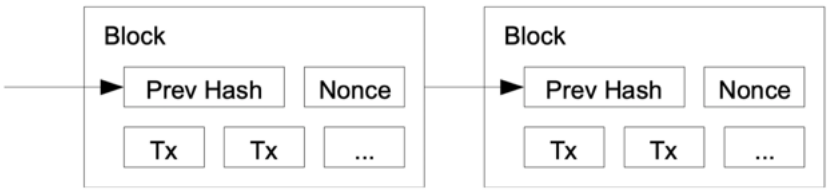
हम जो समाधान पेश कर रहे हैं वह टाइमस्टैम्प से शुरू होता है।टाइमस्टैम्प सर्वर टाइमस्टैम्प किए जाने वाले ब्लॉक[11] के हैश को लेकर तथा उस हैश को व्यापक रूप से प्रकाशित करके कार्य करता है,जैसे समाचार पत्र या यूज़नेट पोस्ट(2-5)।टाइमस्टैम्प प्रमाणित करता है की हैश में दर्ज की गई जानकारी उस समय स्पष्ट और अस्तित्व में रही होगी।प्रत्येक टाइमस्टैम्प इसके हैश में पिछले टाइमस्टैम्प को शामिल कर के एक श्रृंखला बनाता है,जिसमें प्रत्येक अतिरिक्त टाइमस्टैम्प उसके पहले वाले टाइमस्टैम्प को प्रबलित करता है (टाइमस्टैम्प वह जानकारी होती है जो हम बिटकॉइन भेज रहे हैं उनके एड्रेस,उनकी मात्रा,समय,ब्लॉक नंबर और हैश नंबर।यह हैश एक ब्लॉक को अगले ब्लॉक के साथ जोड़ कर एक ब्लॉकचेन बनाता है)।



4. प्रूफ ऑफ़ वर्क
Proof-of-work

पियर-टू-पियर आधार पर वितरित टाइमस्टैम्प सर्वर को चलाने के लिए हमें समाचार पत्र या यूज़नेट पोस्ट के जगह एडम बैक के हैशकैश(6)* जैसी प्रूफ और वर्क प्रणाली का प्रयोग करना होगा(एडम हैशकैश प्रणाली एक क्रिप्टोग्राफी प्रणाली है जिसे एडम कैश नाम के व्यक्ति ने 1997 में पेश किया था ,यह ईमेल स्पेम की सुरक्षा में भी इस्तेमाल होता है)।प्रूफ ऑफ़ वर्क में किसी मूल्य के लिए स्केनिंग करना शामिल होता है जिसे जब हैश किया जाता है,जैसे SHA-256** से,तो हैश अनेक ज़ीरो बिट्स से शुरू होता है।

आवश्यक जीरो बिट्स की संख्या के संदर्भ में जरुरी औसत कार्य कौन कौन से हैं और इसे एक हैश को कार्यान्वित करके सत्यापित किया जा सकता है। हमारे टाइमस्टैम्प नेटवर्क के लिए,हम ब्लॉक के हैश को आवश्यक जीरो बिट्स देने वाला मूल्य न मिल जाए तब तक ब्लॉक में नॉन्स को बढ़ाकर प्रूफ ऑफ़ वर्क को क्रियान्वित करते हैं।



एक बार प्रूफ ऑफ़ वर्क को पूरा कराने के लिए CPU के प्रयास को खर्च कर देने के बाद कार्य को दोबारा किए बिना ब्लॉक को बदला नहीं जा सकता।क्योंकि बाद वाले ब्लॉक पहले वाले ब्लॉक से जोड़ दिए जाते हैं, ब्लॉक को बदलने के काम में उसके बाद वाले सभी ब्लॉक पर दोबारा काम करना शामिल होगा(बिटकॉइन के ब्लॉक में इसकी सुरक्षा जुडी है ,जब एक ब्लॉक में टाइमस्टैम्प द्वारा जानकारिया जोड़ दी जाती है तो इनको बदला नहीं जा सकता)।

प्रूफ ऑफ़ वर्क बहुसंख्या निर्णयन में प्रतिनिधित्व निर्धारित करने की समस्या का भी हल निकालता है।यदि बहुसंख्या वन-IP-एड्रेस-वन-वोट पर आधारित हो,तो उसे कई IPs आबंटित कर सकने वाला कोई व्यक्ति नष्ट कर सकता है।प्रूफ ऑफ़ वर्क मूल रूप से वन-CPU-वन-वोट है।बहुसंख्या निर्णय का प्रतिनिधित्व सबसे लंबी श्रृंखला(सबसे बड़ी ब्लॉकचेन)करती है,जिसमें सबसे ज्यादा प्रूफ-ऑफ़-वर्क प्रयास निवेश किया गया है।

यदि अधिकांश CPU पावर ईमानदार नोड्स द्वारा नियंत्रित होता है,तो ईमानदार श्रृंखला में सबसे तेज़ गति से वृद्धि होगी और वह किसी प्रतिस्पर्धी श्रृंखला से आगे निकल जाएगी(यहां ईमानदार CPU उन लोगों को कहा गया है जो बिटकॉइन की माईनिंग करते हैं)।किसी पिछले ब्लॉक को परिवर्तित करने के लिए हमलावर (अटैकर) को उस ब्लॉक के और उसके बाद वाले ब्लॉक के प्रूफ ऑफ़ वर्क को दोबारा करना होगा और फिर ईमानदार नोड्स के कार्य की बराबरी पर आना होगा और उससे तेज़ और बेहतर काम करना होगा।हम आगे दिखाएंगे कि जैसे जैसे बाद वाले ब्लॉक जोड़े जाते हैं वैसे वैसे धीमे हमलावर की बराबरी पर आने की संभावना धीरे धीरे कम होती जाती है।

भविष्य में हार्डवेयर की गति बढ़ने और नोड्स के संचालन में परिवर्ती रूचि की क्षतिपूर्ति करने के लिए प्रूफ ऑफ़ वर्क की कठिनाई(difficulty)प्रति घंटा ब्लॉक की औसत संख्या को लक्ष्यंकित करने वाला चल औसत निर्धारित करता है।यदि ब्लॉक बहुत तेज़ बनते हैं तो कठिनाई बढ़ जाती है।

5. नेटवर्क
Network

नेटवर्क का संचालन करने के निम्नलिखित कदम हैं:

1.नए लेनदेन(बिटकॉइन ट्रंज़ेक्शन)सभी नोड्स पर प्रसारित किए जाते हैं।
2.प्रत्येक नोड नए लेनदेन को एक ब्लॉक में इकठ्ठा करता है।
3.प्रत्येक नोड अपने ब्लॉक के लिए कठिन प्रूफ ऑफ़ वर्क खोजने पर काम करता है।
4.जब नोड प्रूफ ऑफ़ वर्क को खोज लेता है तो वह ब्लॉक को सभी नोड्स पर प्रसारित करता है।
5.नोड्स तभी ब्लॉक को स्वीकार करते हैं जब सभी लेनदेन मान्य होते हैं और पहले से ही व्यय नहीं किए गए होते।
6.नोड्स स्वीकृत ब्लॉक के हैश को पिछले हैश के रूप में प्रयोग करके श्रृंखला में अगला ब्लॉक बनाने पर कार्य करके उस ब्लॉक की स्वीकृति व्यक्त करते हैं।

नोड्स हमेशा सबसे लंबी श्रृंखला को सही वाली श्रृंखला समझते हैं और उसका विस्तार करने पर कार्य करते रहते हैं।यदि दो नोड्स अगले ब्लॉक के विभिन्न संस्करणों को एक साथ प्रसारित करें,तो कुछ पहले एक या दूसरा प्राप्त कर सकते हैं।इस मामले में वे उन्हें पहले प्राप्त हुए ब्लॉक पर काम करते हैं, लेकिन दूसरी शाखा को सहेज लेते है जब वह लंबी बन जाती है;इसके बाद जो नोड्स दूसरी शाखा पर काम कर रहे थे वे लंबी वाली शाखा पर काम करने लगते हैं।नए लेनदेनों के प्रसारणों को सभी नोड्स पर पहुँचना जरुरी नहीं है।अगर लेनदेन कई नोड्स पर पहुँचते हैं तो वे जल्दी ही किसी ब्लॉक में आ जाएंगे।ब्लॉक का प्रसारण उन संदेशों के लिए सवेंदना रखता है जो रह गए हैं।अगर कोई भी नोड किसी ब्लॉक को नहीं लेता तो अगले ब्लॉक मिलने पर वह पहले ब्लॉक के लिए अनुरोध करेगा और इस से पता चलता है कि एक ब्लॉक रह गया है।(इस एक तकनीक के कारण बिटकॉइन ब्लॉकचेन पर हुआ कोई भी लेनदेन छूट नहीं सकता , हो सकता है की इसमें थोड़ी देर हो जाए लेकिन अगला ब्लॉक लेने से पहले सिस्टम यह बताता है की कोई लेनदेन रह गया है और उसे पूरा करना जरुरी है ।)

6. प्रोत्साहन
Incentive or Block Reward

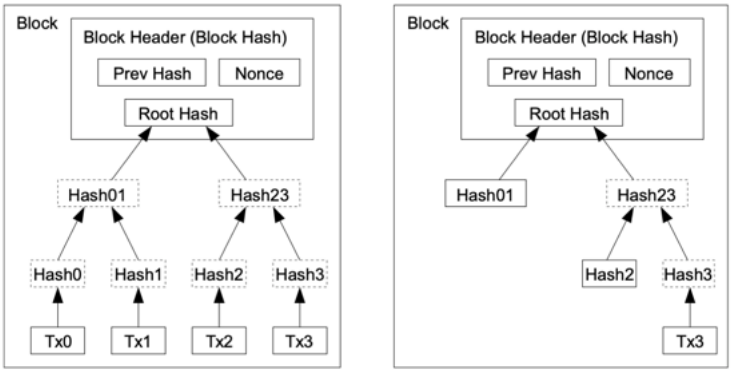
परंपरा के अनुसार ब्लॉक में मौजूद पहला लेनदेन एक विशेष लेनदेन होता है जो ब्लॉक निर्माता के स्वामित्व वाला नया सिक्का शुरू करता है।यह नोड्स का समर्थन करने के लिए प्रोत्साहन (ब्लॉक रिवार्ड)को जोड़ता है,क्योंकि सिक्कों को जारी करने वाला कोई केंद्रीय व्यक्ति नहीं है तो यह प्रारंभिक रूप से सिक्कों को संचालन में डालने का तरीका देता है।अनेक नए सिक्कों को स्थिर रूप से लगातार जोड़ते जाना सोना खनिकों(गोल्ड माइनर)द्वारा सोने को संचालन में डालने के लिए संसाधन खर्च करने के बराबर है।हमारे काम में यह काम CPU समय और विधुत शक्ति है जो बढ़ती है।(यहां पर ब्लॉक को माईनिंग करने वालों को मिलने वाले रिवॉर्ड की बात की गई है और जैसे जैसे यह आगे बढ़ेगा वैसे वैसे CPU समय और बिजली की जरूरत बढ़ेगी)।

प्रोत्साहन[12](ब्लॉक रिवॉर्ड) के लिए धन लेनदेन के लिए दिए जाने वाले शुल्क से भी उपलब्ध कराया जा सकता है।अगर किसी लेनदेन की आउटपुट (उत्पादन)कीमत इनपुट कीमत से कम है,तो इसका अंतर लेनदेन शुल्क है जिसे लेनदेन को शामिल करने वाले ब्लॉक के रिवॉर्ड मूल्य में जोड़ दिया जाता है।एक बार निर्धारित कॉइन पूरी तरह बाजार में आ जाने के बाद लेनदेन पूरी तरह मुद्रास्फीति से मुक्त हो जाता है और पूरी तरह लेनदेन की फीस पर आधारित रह जाता है(जब सारा बिटकॉइन माईन हो कर बाजार में आ जाएगा उसके बाद माईनिंग करने वालों को सिर्फ लेनदेन की फीस पर ही काम करना पड़ेगा)।

प्रोत्साहन(इंसेंटिव)नोड्स को चलाने वालों को ईमानदार रख सकता है।अगर कोई हैकर सभी ईमानदार नोड्स से ज्यादा CPU की ताकत जुटा सकता है तो उसे उसका उपयोग अपने भुगतान चुरा कर लोगों को धोखा देने या उसका उपयोग नए सिक्कों के उत्पादन इन दोनों के बीच चुनाव करना होगा।उसे प्रणाली को और अपने धन की मान्यता को नुक्सान पहुचाने के बजाय, दिए गए नियमो का पालन करना ज्यादा फायदेमंद लगेगा, ऐसा नियम जो उसे अन्य सभी नोड्स से अधिक नए सिक्के उपलब्ध करवाकर उसका समर्थन करें।

7. डिस्क स्पेस पुनः प्राप्त करना
Reclaiming Disk Space

एक बार नए सिक्के का लेनदेन कई ब्लॉक में डाल दिया जाता है,तो डिस्क में जगह बचाने के लिए उससे पहले व्यय किए गए लेनदेनों को हटाया जा सकता है। इसे ब्लॉक के हैश को तोड़े बिना आसान बनाने के लिए ब्लॉक के हैश में केवल रूट को शामिल करके,लेनदेन को मेर्कले ट्री[7][2][5]में हैश किया जाता है। फिर ट्री की शाखाओं को काटकर पुराने ब्लॉक्स को छोटा किया जा सकता है। अंदर के हैश को संग्रहित करने की जरुरत नहीं होती।



Transactions Hashed in a Merkle Tree

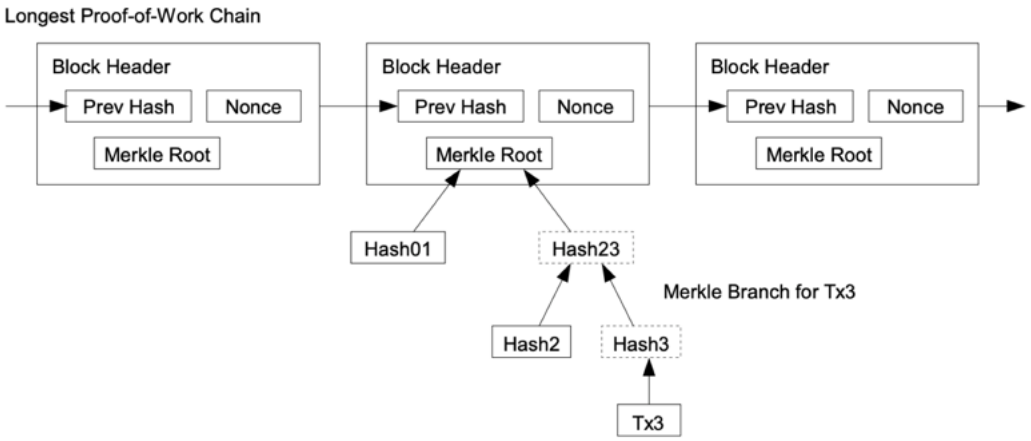
After Pruning Tx0-2 from the Block

कोई भी बिना लेनदेन का ब्लॉक हेडर लगभग 80 बाइट का होगा। अगर हम मान लें कि ब्लॉक हर 10 मिनट में उत्पन होते हैं, तो 80 बाइट *6*24*365*= हर वर्ष 4.2MB.

2008 में आम तौर पर 2GB वाले कंप्यूटर सिस्टम की बिक्री,और नूर के नियम द्वारा की गई हर साल 1.28GB की वर्तमान वृद्धि की भविष्यवाणी को देखते हुए ब्लॉक हेडर्स को मेमरी में रखा जाना जरूरी हो तब भी भण्डारण की कोई समस्या नहीं होनी चाहिए।

8. सरलीकृत या आसान भुगतान सत्यापन
Simplified Payment Verification

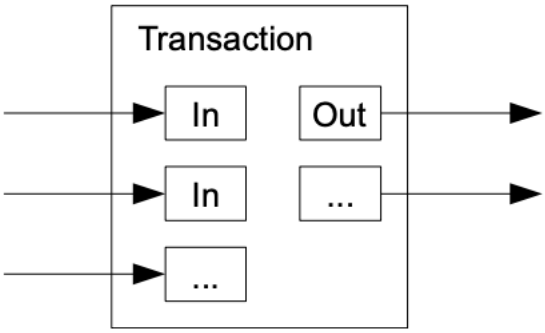
एक संपूर्ण नेटवर्क नोड का संचालन किए बिना भुगतानों को सत्यापित(वेरिफाइड)करना संभव है। उपयोगकर्ताओं को केवल सबसे लंबी प्रूफ ऑफ़ वर्क श्रृंखला के ब्लॉक हेडर्स की एक प्रतिलिपी रखने की जरुरत होती है,जिसे वह तब तक नेटवर्क नोड्स से प्रश्न करके प्राप्त कर सकता है जब तक वह आश्वस्त न हो जाए कि उसके पास सबसे लंबी श्रृंखला है,और उस ब्लॉक से लेनदेन को लिंक करती हुई मर्केल शाखा प्राप्त करने की जरुरत होती है जिसमें उसे टाइम स्टेम्प किया गया है।वह खुद लेनदेन की जाँच नहीं कर सकता लेकिन श्रृंखला में किसी जगह लिंक करके वह देख सकता है कि किसी नेटवर्क नोड ने उसे स्वीकार किया है साथ ही उसके बाद के जोड़े गए ब्लॉक इस बात की पुष्टि करते हैं कि नेटवर्क ने उसे स्वीकार कर लिया है।



इसी कारण सत्यापन तब तक विश्वसनीय होता है जब तक ईमानदार नोड्स नेटवर्क को नियंत्रित करते हैं,लेकिन यदि हमलावर नेटवर्क को नियंत्रण में लेता है तो यह अधिक भेद्द होता है।हलाकि नेटवर्क नोड्स अपने आप लेनदेन की प्रविष्टियों (transaction entry in block)को सत्यापित (वेरिफाई) कर सकते हैं, लेकिन क्रमबद्ध तरीका तब तक हमलावर के जाली लेनदेन के धोखे में आ सकता है जब तक हमलावर नेटवर्क को नियंत्रित करना जारी रखता है।इस से बचने का तरीका यह हो सकता है कि असमान्य ब्लॉक मिलने पर नेटवर्क द्वारा चेतावनी जारी करना और उपयोगकर्ताओं के सॉफ्यवेयर को पूरे ब्लॉक और चेतावनी देने वाले लेनदेन को डाउनलोड करने के लिए प्रेरित करना।लगातार लेनदेन प्राप्त करने वाले व्यवसाय अपने खुद के नोड्स को चलाना जरुरी समझेंगे ताकि अधिक स्वतंत्र,सुरक्षा और जल्द लेनदेन कर सकें।

9. मूल्यों को एक करना और विभाजित करना
Combining and Splitting Value

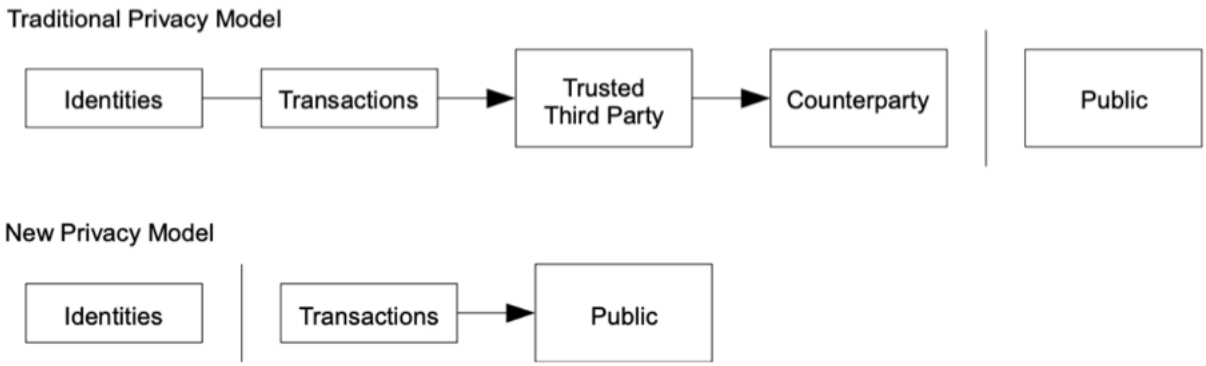
हालांकि सिक्कों का व्यक्तिगत तौर पर प्रबंधन संभव होगा ,फिर भी हर एक सिक्के के लिए अलग लेनदेन बहुत बोझिल[13](unwieldy) हो जाएगा। मूल्यों को अलग करने और एक करने के लिए लेनदेन में कई इनपुट और आउटपुट होते हैं। सामान्यता या तो पिछली बड़ी ट्रांजक्शन से एक अकेला इनपुट होगा या कई इनपुट होंगे छोटे मूल्यों के,या ज्यादा से ज्यादा दो आउटपुट होंगे एक भुगतान के लिए और एक रेजगारी(सिक्के की बहुत छोटी मात्रा) देने वाले को वापिस करने के लिए अगर कोई है तो।



यह ज्ञात रखना चाहिए की एक लेनदेन कई लेनदेनों पर निर्भर करता है,और वह लेनदेन कई और लेनदेनों पर निर्भर करता है लेकिन यह कोई समस्या नहीं है। किसी लेनदेन की पूरी स्टैंडअलोन प्रतिलिपी(वह लेखजोख जिसमें लेनदेनों की जानकारी होती है एक्सल शीट या और और किसी रूप में) निकालने की जरुरत कभी भी नहीं पड़ती।

10. निजता या गोपनीयता
Privacy

पारम्परिक बैंकिंग प्रणाली एक हद तक निजता को प्राप्त कर पाती है ग्रहकों की जानकारी तीसरे पक्ष तक सीमित रख कर कर। सार्वजनिक रूप से सभी लेनदेनों की घोषणा करने की जरुरत इस तरीके को असंभव बना देती है,लेकिन दूसरी जगह जानकारी के प्रवाह को कम करके निजता को बनाए रखा जा सकता है:सार्वजनिक कुंजियों(public key or bitcoin receiving address)को गुमनाम रख कर। आम लोगो यह देख सकते हैं कि किसी ने किसी को धनराशि भेजी है लेकिन किसको ? यह गोपनीय रहेगा[14]। यह शेयर बाजार की तरह कम जानकारी देने की तरह काम करेगा,जहां एक व्यक्ति की ट्रेड के समय और आकार को सार्वजनिक किया जाता है बिना यह बताए की यह किसने किया।



अतिरिक्त सुरक्षा के मध्य नज़र हर एक लेनदेन के लिए नई पब्लिक कुंजियों (public key or receiving address) का प्रयोग करना चाहिए एक ही मालिक की पहचान से बचने के लिए(हर बार अलग पब्लिक की का इस्तेमाल करने से आपकी पुरानी ट्रांजक्शन को नहीं देखा जा सकेगा)।

इसमें खतरा यह है कि अगर एक कुंजी के मालिक का पता चल जाए तो उसके सभी लेनदेन उजागर हो जाएंगे जो उस से सम्बंधित है।

11. गणना
Calculations

हम मुख्य ब्लॉकचेन से अलग एक तेज ब्लॉकचेन की कल्पना करते हैं जिसे हमलावर (attacker)ने बनाया है। अगर इसे स्वीकृत भी कर लिया जाए तब भी प्रणाली को मनमाने बदलाव नहीं करने देगी,जैसे की कीमतों में अचानक बदलाव करना या उस पैसे को ले जाना जो हमलावर का नहीं है। नोड्स ऐसे किसी लेनदेन को स्वीकार नहीं करेंगे जो मान्य न हो और ईमानदार नोड्स ऐसे किसी ब्लॉक को भी स्वीकार नहीं करेंगे जिसमें ऐसे अमान्य लेनदेन की प्रविष्टि हो। हमलावर केवल अपने द्वारा किए गए लेनदेन में व्यय किए गए धन को वापिस लेने के लिए एक लेनदेन को बदलने का प्रयास कर सकता है।

ईमानदार श्रृंखला(honest blockchain) और हमलावर श्रृंखला(attacker chain) की रेस का चित्रण बायनॉमियाल रैंडम वॉक के रूप में किया जा सकता है। सफल घटना है ईमानदार श्रृंखला की बढ़त को +1 से बढ़ाते हुए उसका एक ब्लॉक से विस्तार,और विफल घटना है हमलावर श्रृंखला का -1 के अंतर से एक ब्लॉक का विस्तार होना।

किसी हमलावर की बराबरी पर आने की संभावना किसी जुआरी की बर्बादी की तरह है।मान लें कि किसी जुआरी के पास असीमित ऋण है,और वह मुख्य चेन की बराबरी के लिए अनगिनत चाले चलता है।क्या वह कभी भी मुख्य चेन तक पंहुच पाएगा यह हम इस उदहारण से समझते हैं

P: ईमानदार नोड अगला ब्लॉक खोज लेगा इसकी सम्भावना
q: हमलावर अगला ब्लॉक खोज लेगा इसकी सम्भावना
qz: हमलावर कभी भी z ब्लॉक्स पीछे से बराबरी पर आएगा इसकी सम्भावना

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

हमारे अनुसार यहां p>q है,हमलावर को जिन ब्लॉक के बराबर आना है उनकी संख्या में वृद्धि होने के साथ संभावना घातीय रूप से कम हो जाती है।मुश्किलों (difficulty of mining)का सामना करते हुए,यदि वह शुरू में ही किस्मत से आगे नहीं बढ़ जाता,तो उसके और पीछे छूट जाने की संभावनाएं बहुत कम होती जाती है।

अब हम इस बात को देखते हैं कि किसी ट्रांजक्शन को प्राप्त करने वाला कितनी देर इंतजार करे यह विश्वास करने का की भेजने वाला इस लेनदेन को बदल न सके?हम मान लेते हैं कि भेजने वाला हमलावर है और वह प्राप्तकर्ता को कुछ देर के लिए यह विश्व दिलाना चाहता है कि उसने भुगतान कर दिया,और कुछ समय के बाद वह उस भुगतान को बदल देता है।जब कभी ऐसा होगा तो प्राप्तकर्ता को चेताया जाएगा,लेकिन भेजने वाला यह उम्मीद करता है कि इसमें बहुत देर हो गयी।

प्राप्त करने वाला हस्ताक्षर करने से पहले कुंजी (Key) की एक नई जोड़ी(public key, private key)बनाता है और सार्वजनिक की(public address) भेजने वाले को देता है।यह क्रिया भेजने वाले हमलावर को बहुत आगे बढ़ने,समय से पहले ब्लॉक बना कर लेनदेन को क्रियान्वित करने से रोकता है।एक बार लेनदेन को भेजने के बाद भेजने वाला हमलावर समानांतर चेन पर गुप्त रूप से काम करने लगता है,जिसमें उसके लेनदेन का वैकल्पिक संस्करण होता है।

प्राप्तकर्ता तब तक प्रतीक्षा करता है जब तक लेनदेन को ब्लॉक में जोड़ा नहीं जाता और उसके बाद z ब्लॉक्स लिंक नहीं किए जाते।प्राप्तकर्ता नहीं जानता हमलावर ने कितनी प्रगति की है,लेकिन यह मानकर की ईमानदार ब्लॉक्स ने प्रति ब्लॉक औसत अपेक्षित समय लिया है,हमलावर की संभावित प्रगति पॉसों वितरण होगी जिसका अपेक्षित मूल्य होगा:

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

हमलावर अभी भी बराबरी पर आ सकता है इसकी सम्भावना प्राप्त करने के लिए हम उस बिंदु जहां से वह बराबरी पर आ सकता है इसकी सम्भावना का,उस प्रगति के प्रत्येक मात्रा के पॉसों घनत्व से गुणा करते हैं जो वह कर सकता है:

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

अपरिमित वितरण तल का जोड़ लगाने से बचने के लिए पुनः व्यवस्था करते हुए-

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

C कोड में रूपान्तरित करते 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 परिणामो को चलाकर,हम देख सकते हैं कि z के साथ संभावना घातीय रूप से कम होती 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

1.1 से कम P के लिए हल निकालते हुए-
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

निष्कर्ष
Conclusion

हमने विश्वास पर निर्भर हुए बिना इलेक्ट्रॉनिक लेनदेनों के लिए एक प्रणाली पेश की है। हमने डिजिटल हस्ताक्षरों से बने सिक्कों के साधारण ढांचे से शुरुआत की,जो स्वामित्व पर मजबूत नियंत्रण प्रदान करता है,लेकिन जो दोहरे-व्यय को रोकने के तरीके के बिना अपूर्ण है। इसका हल निकालने के लिए हमने लेनदेनों के सार्वजनिक इतिहास को दर्ज करने के लिए प्रूफ ऑफ़ वर्क को उपयोग करके पियर-टू-पियर नेटवर्क पेश किया,जिसे बदलना हमलावर के लिए संगठन की दृष्टि से शीघ्र ही अव्यवहारिक बन जाता है,यदि ईमानदार नोड्स अधिकांश CPU पावर को नियंत्रित करें। नेटवर्क अपनी संचारित सरलता में मजबूत है।

थोड़े समन्वय के साथ सभी नोड्स एक ही समय पर काम करते हैं। इनकी पहचान नहीं करनी पड़ती,क्योंकि संदेश किसी खास जगह नहीं भेजे जाते और उन्हें केवल श्रेष्ठ प्रयास के आधार पर पहुचाना होता है। नोड्स अपनी अनुपस्थिति में जो हुआ उसके प्रमाण के रूप में प्रूफ-ऑफ़-स्टेक की श्रृंखला को स्वीकार करके,इच्छानुसार नेटवर्क को छोड़ सकते हैं और इसमें फिर से जुड़ सकते हैं। नोड्स मान्य ब्लॉक्स को स्वीकार करके आगे बढ़ाने के लिए और अमान्य ब्लॉक्स पर कार्य करने से इंकार कर उसे अस्वीकार करके अपने CPU पावर से वोट कर सकते हैं। सहमति की इस क्रियाविधि से किसी भी आवश्यक नियम और प्रोत्साहन को प्रवर्तित किया जा सकता है।

यहाँ ऊपर दिए गए कठिन शब्दों या न समझ आने वाली पंक्तियों को समझाने की कोशिश की गई है। यहाँ से पढ़ कर आप ऊपर लिखी गई पंक्तियों या शब्दों को बेहतर तरीके से समझ सकते हैं।

1.बिटकॉइन के नेटवर्क को किसी एक या किसी खास सर्वर से नहीं चलाया जाता। इसका फायदा यह है कि एक जगह अगर कोई समस्या आ भी जाए तब भी बिटकॉइन नेटवर्क सुचारू रूप से चलता रहेगा।

2. इस वाइट पेपर में कई जगह 'लेनदेन' शब्द का इस्तेमाल होगा जिसके अर्थ बिटकॉइन के लेनदेन से है।

3. श्रृंखला ब्लॉकचेन blockchain को कहा गया है।

4. लेनदेन की प्रविष्टियां-बिटकॉइन की ट्रांजक्शन का ब्लॉकचेन में दर्ज होना या रिकॉर्ड होना।

5.टाइम स्टैम्प-जिस समय ट्रांजक्शन की गई, उसकी कीमत,फीस,ब्लॉक नंबर और ट्रांजक्शन हैश के साथ ही किस एड्रेस से किस एड्रेस पर बिटकॉइन को भेजा गया यह सारी जानकारी टाइम स्टैम्प में दर्ज होगी।

6.वह कंप्यूटर और CPU जो बिटकॉइन की ट्रांजक्शन को सत्यापित वेरिफाई करने का काम करते हैं।

7.हमलावर वह है जो बिटकॉइन की ब्लॉकचेन से छेड़ छाड़ करना चाहते हैं और इसकी ब्लॉकचेन को नुक्सान पहुँचाना चाहते है।

8.ईमानदार नोड्स वह UCP ऑपरेटर हैं जो असली ब्लॉकचेन को सफलतापूर्वक चलाने में सहयोग करते हैं।

9. इलेक्ट्रॉनिक कोइन बिटकॉइन Bitcoin को कहा गया है।

10.टक्साल यानि बिटकॉइन माईनिंग करने वाले।

11.ब्लॉक बिटकॉइन ब्लॉकचेन का सबसे मुख्य भाग है।यह एक कॉपी की तरह है जिसमें बिटकॉइन के सभी लेनदेन दर्ज होते हैं और फिर माईनिंग करने वालों के पास जाते है और वह हर ब्लॉक की ट्रांजक्शन की जाँच करके उसे सही एड्रेस तक पहुँचाते हैं।

12.प्रोत्साहन या ब्लॉक रिवॉर्ड वह है जो बिटकॉइन माईनिंग करने वालों को अपना काम करने के बदले मिलता है।बिटकॉइन का एक ब्लॉक 10 मिनट में बनता है और इसको माईन करने वालों को इसके बदले में बिटकॉइन मिलता है इस तरह से हर 10 मिनट में नया बिटकॉइन बाजार में आता है।2020 में हर एक बिटकॉइन ब्लॉक को माईन करने पर 6.25 बिटकॉइन मिल रहा है जो 2024 में आधा रह जाएगा और यह तब तक होगा जब तक सभी 2 करोड़ 10 लाख बिटकॉइन नहीं बन जाते।

13. unwieldy का मतलब होता है बोझिल जिसका अर्थ होता है धीमा ,आहिस्ता ,सुस्त और यहाँ इसका अर्थ है की अगर हर एक लेनदेन के लिए अलग अलग रख रखाव करना पड़े तो यह बहुत मुश्किल होगा और सुस्त भी होगा यानि धीमा होगा।

14. बैंक में किसी भी तरह का लेनदेन करने के लिए दोनों पक्षों को अपनी सारी निजी जानकारी तीसरे पक्ष यानि बैंक को देनी जरुरी है,लेकिन बिटकॉइन नेटवर्क में यह जरुरी नहीं है , हालांकि पारदर्शिता के लिए सभी लेनदेन ऑनलाइन देखे जा सकते हैं लेकिन बिटकॉइन एड्रेस से व्यक्ति की पहचान छुपी रहती है।

*एडम बैक के हैशकैश को यहाँ पढ़ें https://en.wikipedia.org/wiki/Hashcash
**SHA256 को यहाँ पढ़ें https://en.wikipedia.org/wiki/SHA-2

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.

सहयोगी