Shodh International: A Multidisciplinary International Journal (In Hindi)
https://www.eurekajournals.com/shodh.html
ISSN: 2581-3501

बिटकॉइन और ब्लॉक श्रृंखला में स्वामित्व क्रिप्टोग्राफ़िक कुंजियों द्वारा निर्धारित किया जाता है।

डॉ. अजय कृष्ण तिवारी[1]

[1]शिक्षाविद और अर्थशास्त्री और पीएच.डी. मार्गदर्शक

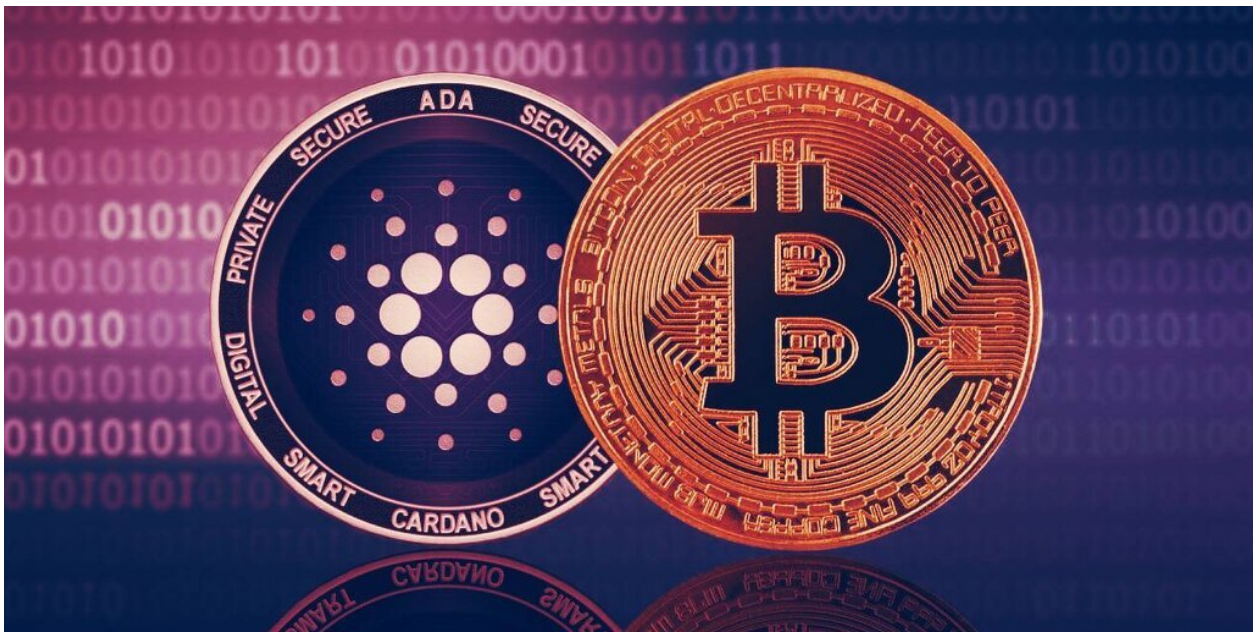
सार

बिटकॉइन ब्लॉक श्रृंखला में दो प्रकार की मालिकाना क्रिप्टोग्राफ़िक कुंजियों का एक विशेष गणितीय संबंध है जो उन्हें डिजिटल संदेशों पर हस्ताक्षर करने के लिए उपयोगी बनाता है। यहां बताया गया है कि यह कैसे होता है: हेल्मुट एक संदेश लेता है, इसे जोड़ता है। पहला, जिसे सार्वजनिक कुंजी कहा जाता है, किसी के देखने के लिए ब्लॉकचेन पर रहता है। दूसरी निजी कुंजी है, और इसका स्वामी इसे दूसरों की दृष्टि से सुरक्षित रखता है। आपकी निजी कुंजी के साथ, कुछ गणनाएँ करता है, और एक लंबी संख्या के साथ समाप्त होता है। कोई भी व्यक्ति जिसके पास मूल संदेश है और संबंधित सार्वजनिक कुंजी जानता है, यह सत्यापित करने के लिए कि लंबी संख्या निजी कुंजी के साथ बनाई गई थी, स्वयं की कुछ गणना कर सकता है। बिटकॉइन में, लेन-देन को निजी कुंजी के साथ हस्ताक्षरित किया जाता है, जो हाल ही में खर्च किए गए सिक्कों से जुड़ी सार्वजनिक कुंजी से मेल खाती है। और जब लेन-देन संसाधित हो जाता है, तो उन सिक्कों को एक नई सार्वजनिक कुंजी सौंपी जाती है।

कीवर्ड: बिटकॉइन, क्रिप्टोग्राफ़िक कुंजियाँ, ब्लॉक चेन, गुमनाम रूप से, कंप्यूटिंग शक्ति, एल्गोरिथम।

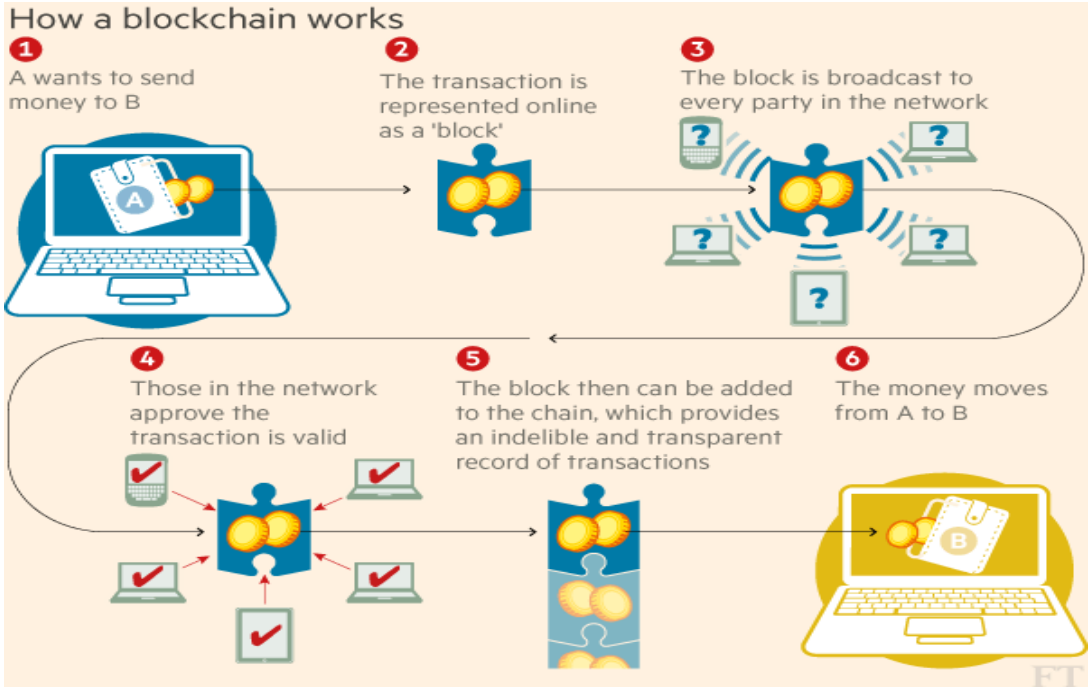
परिचय

खनिकों की मुख्य भूमिका नए लेनदेन की अपरिवर्तनीयता सुनिश्चित करना है, जिससे उन्हें अंतिम और अपुष्ट किया जा सके। ऐसा करने के लिए वे जिस विधि का उपयोग करते हैं, उसे सतोशी ताकेमोटो - जो कोई भी है - ने कंप्यूटिंग के क्षेत्र में सबसे महत्वपूर्ण योगदान माना है। अपरिवर्तनीयता की गारंटी तभी आवश्यक हो जाती है जब सभी को और सभी को बही के सत्यापन में भाग लेने के लिए आमंत्रित किया जाता है। यदि बिटकॉइन ब्लॉक श्रृंखला को एक ही बैंक द्वारा प्रबंधित किया जा रहा था, जो एक ही अधिकार क्षेत्र के तहत सत्यापनकर्ताओं के एक सेट के साथ काम कर रहा था, तो लेन-देन करने का तरीका उतना ही सरल होगा जितना कि कंपनी की नीति में निर्धारित किया गया है। और ऐसे में सिर्फ नियमों का पालन न करने वालों को सजा देना जरूरी होगा।



बिटकॉइन में नियमों को लागू करने के लिए कोई केंद्रीय प्राधिकरण नहीं है।

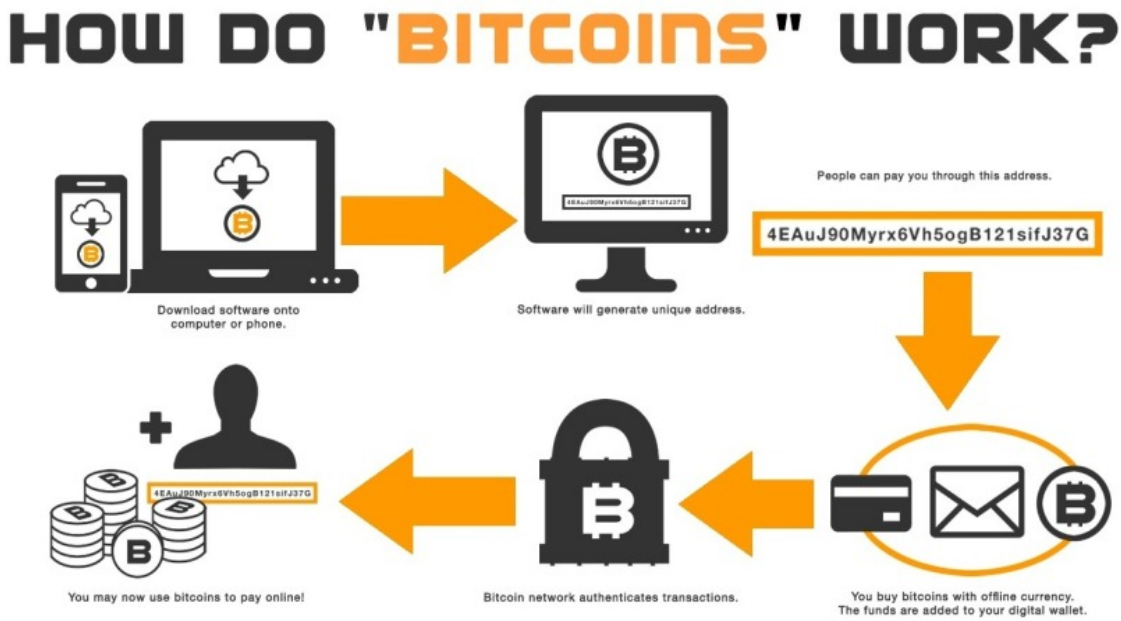
खनिक दुनिया भर में गुमनाम रूप से काम कर रहे हैं - चीन, पूर्वी यूरोप, आइसलैंड, वेनेजुएला में- विभिन्न संस्कृतियों द्वारा शासित और विभिन्न कानूनी प्रणालियों और नियामक दायित्वों के अधीन। इसलिए, उन्हें जवाबदेह ठहराने का कोई तरीका नहीं है। बिटकॉइन कोड पर्याप्त होना चाहिए। ऐसा करने के लिए, बिटकॉइन कार्य के प्रमाण नामक एक योजना का उपयोग करता है और इसके साथ उचित व्यवहार सुनिश्चित करता है। कार्य का प्रमाण ब्लॉक श्रृंखला को कैसे सुरक्षित करता है? सबसे पहले, उस समस्या के बारे में थोड़ा और विशिष्ट रूप से जानें, जिसे सार्वजनिक ब्लॉकचेन काम के प्रमाण के साथ हल करने की कोशिश कर रहे हैं। इस खुले, पीयर-टू-पीयर नेटवर्क में, खनिक- जो कोई भी बिटकॉइन कोड चला रहा है- लेनदेन समाचार प्राप्त करता है और एक नया ब्लॉक बनाने के लिए इसे इकट्ठा करता है। वे एक दूसरे के साथ प्रतिस्पर्धा में ऐसा कर रहे हैं, क्योंकि एक वैध ब्लॉक बनाने वाले पहले व्यक्ति को उस सेवा के लिए (बिटकॉइन में) भुगतान किया जाता है।



बिटकॉइन माइनिंग सॉफ्टवेयर

इस स्थिति को देखते हुए ब्लॉक श्रृंखला में जोड़े जाने के बाद किसी खनिक को पिछले लेनदेन को हटाने से क्या रोक सकता है? जबकि इस प्रकार की फेरबदल एक खनिक को सिक्के चुराने की अनुमति नहीं देता है, इसका उपयोग एक ही सिक्के को कई बार खर्च करने के लिए किया जा सकता है। उदाहरण के लिए, आप बिना देखे किसी व्यापारी के पास जा सकते हैं और बिटकॉइन के साथ एक कप कॉफी के लिए भुगतान कर सकते हैं। यदि मैं एक खनिक होता, तो मैं बाद में बिटकॉइन श्रृंखला के अपने

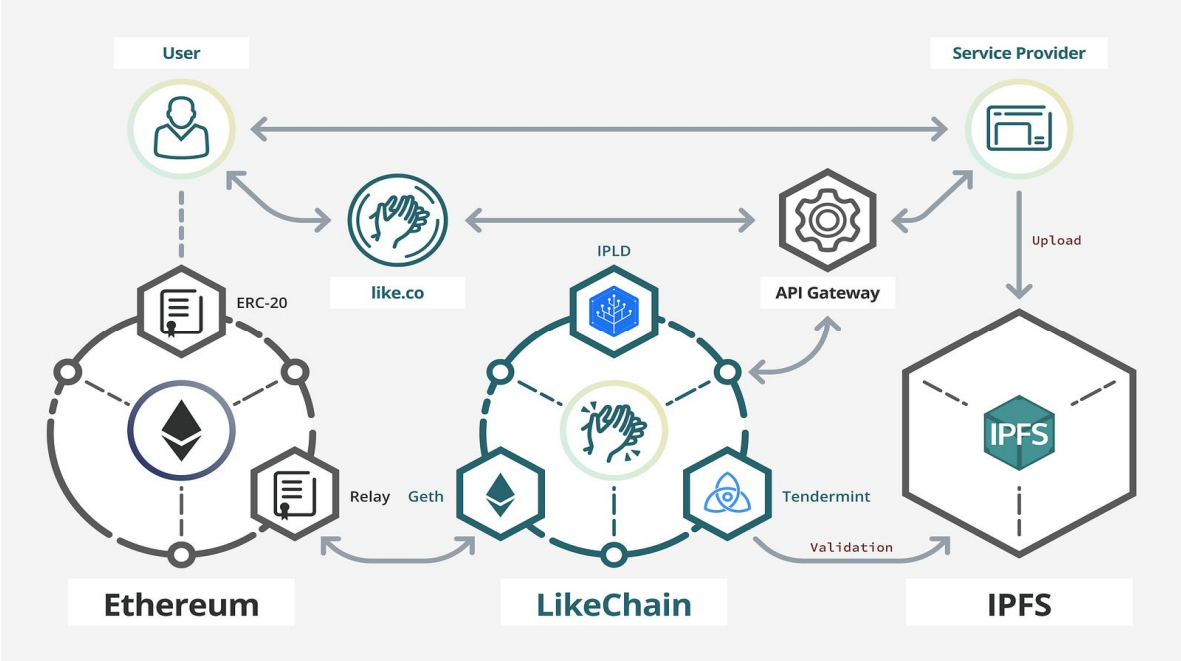
संस्करण पर जा सकता था, लेन-देन को हटा सकता था, और संशोधित श्रृंखला को अपने साथियों को भेज सकता था, इस प्रकार बिटकॉइन को मैंने अपनी जेब में रखा था। दोबारा जमा किया। इसलिए, यह महत्वपूर्ण है कि बिटकॉइन नेटवर्क पर सभी खनिकों के पास ब्लॉक श्रृंखला की एक ही प्रति हो और सभी परिवर्तन और लेनदेन अपरिवर्तनीय हों। एक नया ब्लॉक जोड़ने की कोशिश करने वाले किसी भी खनिक को इसके साथ जाने के लिए एक क्रिप्टोग्राफ़िक प्रमाण भी देना होगा। सबूत उत्पन्न करने के लिए, खनिक हैश फ़ंक्शन के कई दौरों के माध्यम से नए ब्लॉक को पचाता है - एक गणना जो मनमाने ढंग से लंबाई के डेटा का एक टुकड़ा लेती है और इसे एक निश्चित लंबाई के अर्थहीन अल्फ़ान्यूमेरिक स्ट्रिंग में कम कर देती है, जिसे हैश कहा जाता है। प्रक्रिया को और अधिक कठिन बनाने के लिए, ब्लॉक श्रृंखला एल्गोरिथ्म के लिए आवश्यक है कि परिणामी हैश एक निश्चित संख्या में शून्य से शुरू हो। कठिनाई इस तथ्य से आती है कि भविष्यवाणी करने का कोई तरीका नहीं है कि कौन सा हैश डेटा के किसी भी सेट को वापस कर देगा, और इसलिए खनिक बार-बार अपने वैध ब्लॉकों की गणना करते हैं, हर बार जब वे डेटा सेट में एक यादृच्छिक संख्या हिट करते हैं। मान लीजिए, जब वह संख्या बदली जाती है, तो आपको एक नया परिणाम मिलता है। फ़ंक्शन समाप्त हो जाता है जब खनिक अंततः शून्य की सही संख्या प्राप्त करते हैं।



ब्लॉक चेन का पूर्ण संस्करण

एक संतोषजनक हैश खोजने वाला पहला खनिक दूसरे खनिकों को नए ब्लॉक की घोषणा करता है, जो इसकी जांच करते हैं और इसे ब्लॉक श्रृंखला के पूर्ण संस्करण में जोड़ते हैं जो वे अपने कंप्यूटर पर होस्ट कर रहे हैं। यह सब काम करने के लिए, खनिक नए बने बिटकॉइन के साथ-साथ खनन शुल्क का

इनाम इकट्ठा करते हैं, जो ऑपरेशन के शीर्ष पर आने की उम्मीद में उपयोगकर्ता स्वेच्छा से अपने लेनदेन में चुनते हैं। हैशिंग को एक श्रृंखला में ब्लॉक को बंद करने का एक तरीका माना जाना चाहिए। मान लें कि आपके पास एक ताला है जिसे बंद करने के लिए एक चाबी की आवश्यकता है, और आपके पास अपने निपटान में चाबियों का एक बड़ा ढेर है, लेकिन आप नहीं जानते कि कौन सा ठीक से काम करेगा। आपको एक-एक करके प्रयास करना होगा। जब अंत में सही कुंजी मिल जाती है, तो उसे ताले में छोड़ दिया जाता है ताकि कोई भी यह जांच सके कि यह सही है या नहीं।



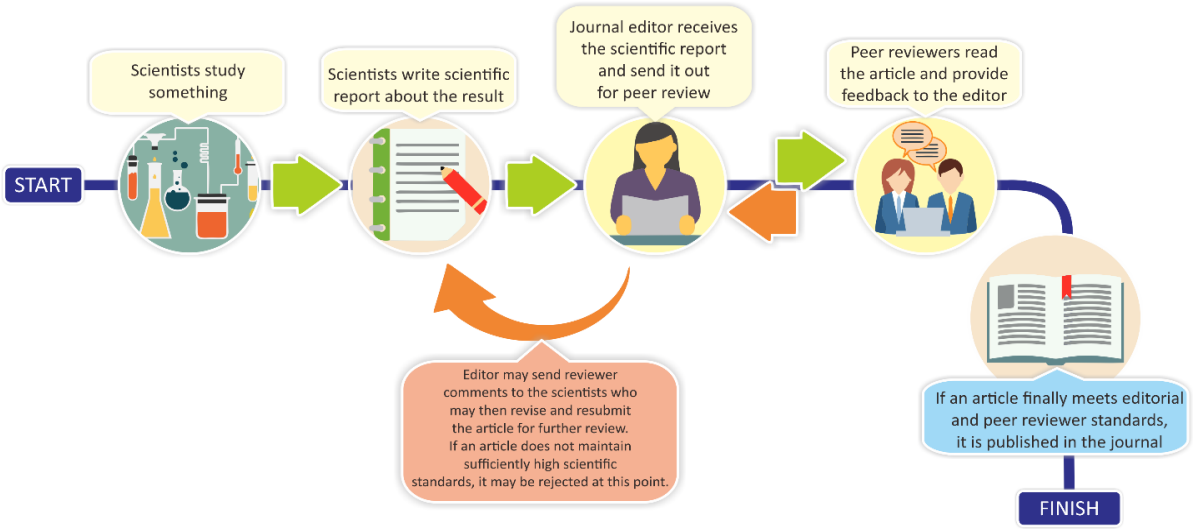
बिटकॉइन खनिक उनके द्वारा प्रदान किए जाने वाले नेटवर्क में भारी निवेश करते हैं

सैद्धांतिक रूप से, यह काम और खनिकों को मिलने वाले पुरस्कार अच्छे व्यवहार के लिए प्रोत्साहन के रूप में काम करते हैं। बिटकॉइन खनिकों को उनके द्वारा प्रदान किए जाने वाले नेटवर्क में भारी निवेश किया जाता है, दोनों बिजली की खपत और उनके द्वारा खरीदे जाने वाले हार्डवेयर में। इसलिए, उनसे किसी भी तरह से मुद्रा को नुकसान पहुंचानेके लिए प्रोत्साहन की कमी की उम्मीद की जाती है, यहां तक कि कोई भी कार्रवाई (जैसे दोहराखर्च) करने से जो बिटकॉइन की अखंडता पर सवाल उठा सकता है और मुद्रा का अवमूल्यन कर सकता है। इस तरह के हमलों को और हतोत्साहित किया जाता है, क्योंकि पुराने ब्लॉकों की सामग्री को बदलने की लागत श्रृंखला में जोड़े गए प्रत्येक नए ब्लॉक के साथ बढ़ जाती है। जब एक नया ब्लॉक बनाया जाता है, तो इसमें पिछले वाले का हैश होता है। पुराने ब्लॉकों में कोई भी परिवर्तन बाद के सभी ब्लॉकों के लिए अमान्य हैश का परिणाम देगा। इसलिए, उस ब्लॉक के बाद किए गए सभी कार्यों को दोहराए बिना पिछले ब्लॉक में डमी मोड सम्मिलित करना

असंभव है। उस लॉक सादृश्य में, यह ऐसा है जैसे श्रृंखला के अंत में लॉक के लिए डिज़ाइन उन सभी तालों पर निर्भर करता है जो इससे पहले आए थे। इसलिए ब्लॉक चेन के बीच में लॉक बदलने का मतलब है कि प्रत्येक बाद के ब्लॉक के लिए नई चाबियां ढूंढनी होंगी।

पहली व्यवहार्य पीयर-टू-पीयर डिजिटल मुद्रा बनाई

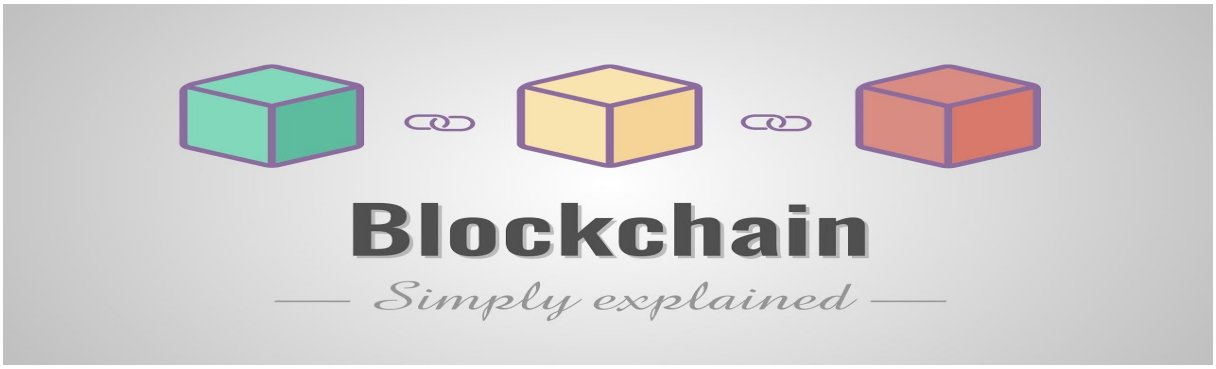
खनिकों को महंगे प्रमाण प्रदान करने के लिए मजबूर करके और फिर उन्हें उनके काम के लिए पुरस्कृत करके, सातोशी ने पहली व्यवहार्य पीयर-टू-पीयर डिजिटल मुद्रा बनाई। लेकिन इसने एक अधिक सामान्य समस्या को भी हल किया जो दशकों से कंप्यूटर वैज्ञानिकों को परेशान कर रही थी: आम सहमति। बिटकॉइन आठ साल पहले किसी भी लम्बाई के लिए कभी भी ऑफ़लाइन नहीं रहा, क्योंकि यह लेनदेन को संसाधित करने और उन घटनाओं के एकल संस्करण को सुनिश्चित करने के लिए (हाँ, संभावित रूप से दुष्ट) प्रतिभागियों के एक नेटवर्क को मज़बूती से प्रोत्साहित करता है। . परिणाम डेटा की एक सतत बढ़ती सरणी है, जिसका निरीक्षण किया जा सकता है और इंटरनेट कनेक्शन वाले किसी भी व्यक्ति द्वारा एकत्र किया जा सकता है, और जो हमला करने के लिए उल्लेखनीय रूप से अभेद्य साबित हुआ है। क्रिप्टोग्राफी एंड कॉन्ट्रैक्ट्स कॉर्नेल यूनिवर्सिटी (IC3) के लिए पहल के सह-निदेशक मीन गन सेरर कहते हैं, बिटकॉइन "दुरुपयोग करने वाली पार्टियों को रोकता है, क्योंकि नुकसान करने वाली पार्टी [कंप्यूटिंग] शक्ति की मात्रा तक सीमित हो सकती है।"



अन्य काम करने के लिए ब्लॉक चेन का उपयोग कैसे करें?

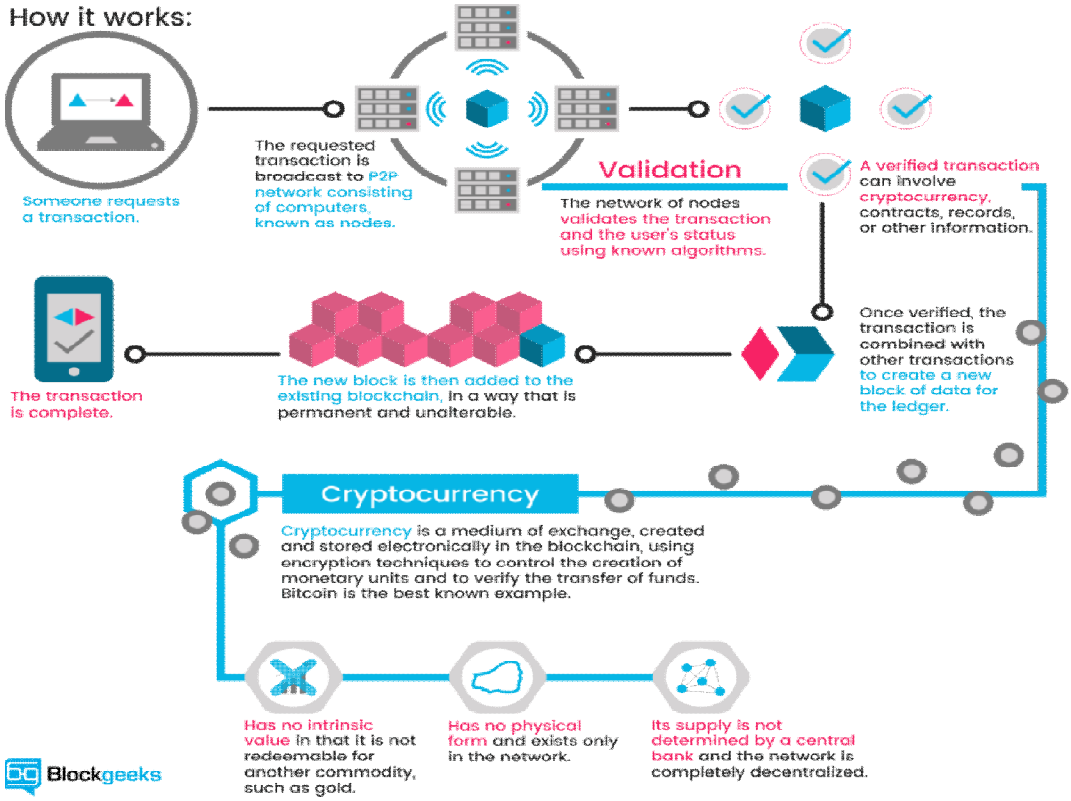
यह पता चला है कि ऐसी प्रणाली सिर्फ पैसे से कहीं ज्यादा उपयोगी हो सकती है। लगभग जैसे ही बिटकॉइन पेश किया गया, लोगों ने कल्पना करना शुरू कर दिया कि ब्लॉक श्रृंखला पर अन्य प्रकार के अनुप्रयोग कैसे चल सकते हैं, और तकनीक व्यापक हो गई। जब खनिक लेन-देन को मान्य करते हैं, तो वे वास्तव में छोटे प्रोग्राम चला रहे होते हैं जो डेटा को क्रंच करते हैं और लेनदेन अनुरोध पर थम्स अप या थम्स डाउन की पेशकश करते हैं। लेकिन क्या होगा अगर वे अधिक जटिल प्रोग्राम चला सकें, जैसे कि सोशल मीडिया नेटवर्क के लिए सॉफ्टवेयर? क्या होगा यदि ब्लॉकचेन का उपयोग साधारण मौद्रिक लेनदेन के अलावा अन्य डेटा का प्रतिनिधित्व करने के लिए किया जाता है, जैसे कि ऑनलाइन फोरम पर संदेश?

हालाँकि ये विचार बिटकॉइन के निर्माण के समय के आसपास थे, टोरंटो में एक 19 वर्षीय कंप्यूटर विज्ञान के छात्र को उन्हें लोकप्रिय बनाने में कई साल लग गए। 2013 में, विटाली ब्यूटिरिन ईथर नामक एक पूरी तरह से नई ब्लॉक श्रृंखला के साथ आया था। थोरियम का लक्ष्य है कि बिटकॉइन ने मुद्रा के रूप में क्या किया और इसे अन्य क्षेत्रों में विस्तारित किया।



बिटकॉइन की तरह, एथेरियम एक ब्लॉक चेन का उपयोग करता है

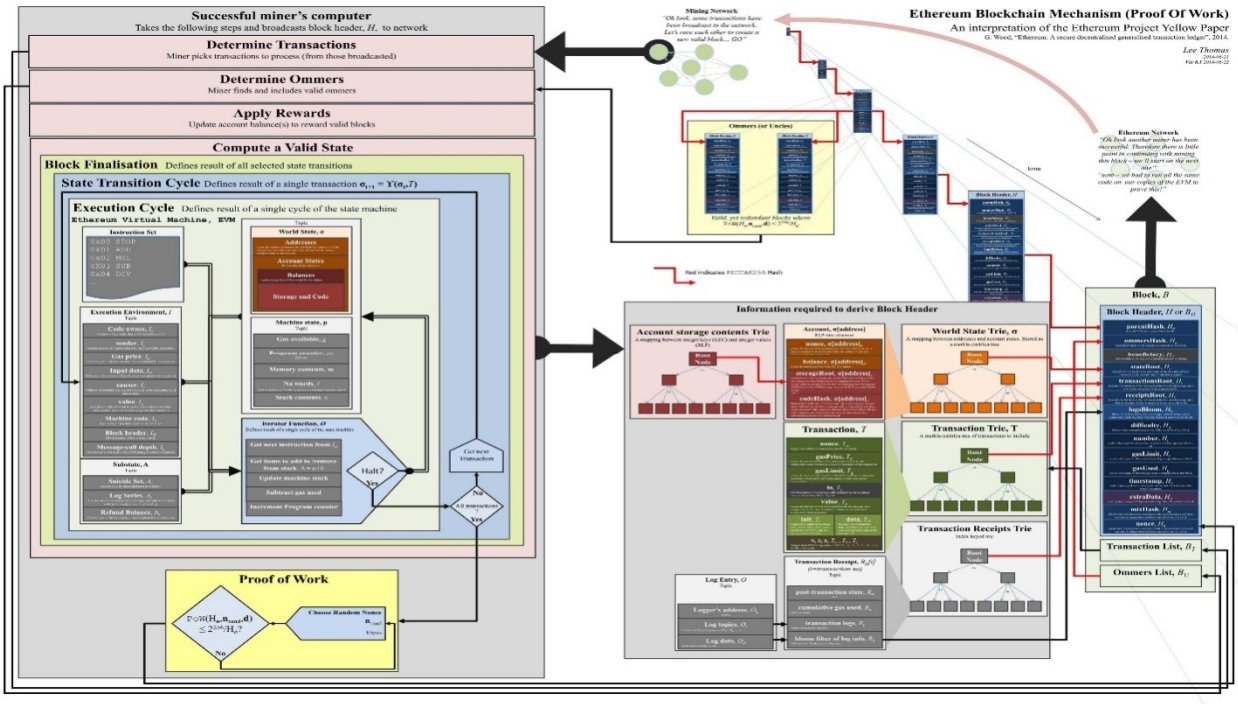
बिटकॉइन की तरह, एथेरियम एक ब्लॉक श्रृंखला का उपयोग करता है जिसकी अपनी मुद्रा होती है, जिसे ईथर कहा जाता है। बिटकॉइन के विपरीत, एथेरियम ऐसे लेन-देन का उपयोग करता है जो मिनी-प्रोग्राम हैं, जिन्हें स्मार्ट कॉन्ट्रैक्ट कहा जाता है जो असीमित मात्रा में जटिल लेखन की मेजबानी कर सकते हैं। उपयोगकर्ता उन्हें निर्देश-युक्त लेनदेन भेजकर प्रोग्राम के साथ इंटरैक्ट कर सकते हैं, जिसे खनिक तब संसाधित करते हैं। व्यवहार में, इसका मतलब है कि कोई भी एक सॉफ्टवेयर प्रोग्राम को लेनदेन में एम्बेड कर सकता है और जानता है कि यह ब्लॉक श्रृंखला के जीवन के लिए अपरिवर्तित और सुलभ रहेगा। सैद्धांतिक रूप से, एथेरियम के साथ आप Facebook, Twitter, Uber, Spotify, या किसी भी अन्य डिजिटल सेवा को नए संस्करणों से बदल सकते हैं जो सेंसर के लिए अभेद्य और उनकी नीतियों में पारदर्शी होंगे, और उन्हें बनाने वाले लोगों की अनुपस्थिति में अस्थिर होंगे। मरते दम तक काम कर सकता है।



बिटकॉइन और एथेरियम जैसी ब्लॉक श्रृंखलाओं की खुली संरचना

"आश्चर्यजनक बात यह है कि आप उस नेटवर्क पर एक कंप्यूटर प्रोग्राम डाल सकते हैं ... और बिटकॉइन की तरह, सिस्टम में हर कोई एक आम सहमति स्थापित कर सकता है कि वास्तव में क्या हु आऔर कब हु आ... मुझे लगता है कि यह एक गहरी अंतर्दृष्टि है," के संस्थापक जोसेफ लुबिंग कहते

हैं एथेरियम, जो अब ब्रुकलिन-आधारित विकेन्द्रीकृत ऐप इनक्यूबेटर आम सहमति चलाता है। अनुमति प्राप्त बहीखाता क्या है? विश्व स्तरीय कंप्यूटर बनाने के लिए ब्लॉक चेन प्रौद्योगिकी का उपयोग करने के लिए ब्यूटिरिन के प्रयास एक अन्य प्रवृत्ति प्रौद्योगिकी को विपरीत दिशा में धकेल रही थी, एक अधिक बंद और सतोशी की उत्कृष्ट कृति का नियंत्रित पुनरावृति। सितंबर 2014 में, वित्तीय संस्थानों के एक समूह - जिसमें बार्कलेज, गोल्डमैन सैक्स और जेपी मॉर्गन शामिल थे - ने R3 नामक एक संघ का गठन किया, यह पता लगाने के लिए कि यह बैंकों के बीच भुगतान की दक्षता में सुधार कैसे कर सकता है। वॉल स्ट्रीट फर्मों को पढ़ने के लिए]। संस्थानों को यह महसूस करने में देर नहीं लगी कि बिटकॉइन ब्लॉक चेन की खुली संरचना जैसे कि कॉइन और एथेरियम उनकी जरूरतों के खिलाफ काम करते हैं। सर्वोपरि चिंता उपयोगकर्ताओं की गुमनामी थी, जिन्हें अल्फ़ान्यूमेरिक पब्लिक एड्रेस द्वारा ओपन ब्लॉक चेन में दर्शाया गया है। उनकी वास्तविक दुनिया की पहचान का कोई संकेत दिए बिना।



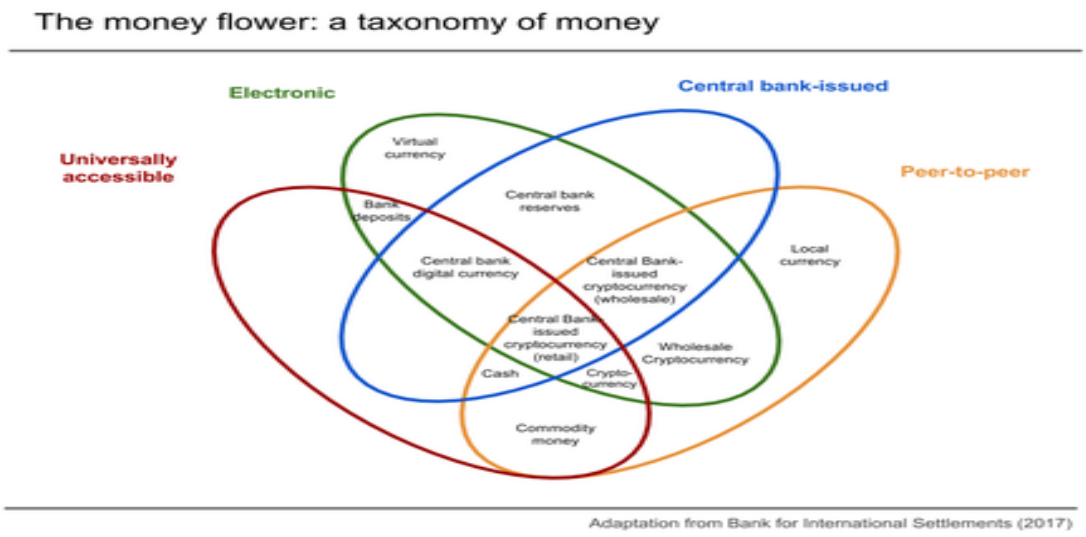
वित्तीय संस्थान कानूनी रूप से ग्राहक डेटा की रक्षा करते हैं

संयुक्त राज्य अमेरिका और अन्य जगहों पर बैंकिंग कानून ऐसी गुमनामी को प्रतिबंधित करते हैं। R3 के लिए मार्केट रिसर्च के निदेशक टिम स्वानसन कहते हैं, "हमें विशेष रूप से यह जानने की जरूरत है कि इन प्लेटफॉर्म पर हमारे प्रतिभागी और प्रतिपक्ष कौन हैं।" वित्तीय संस्थानों को कानूनी रूप से ग्राहक डेटा की रक्षा करने और अपनी संपत्ति और राष्ट्रीय या क्षेत्रीय लाइनों में निर्यात किए गए डेटा को नियंत्रित करने की भी आवश्यकता होती है। क्योंकि सार्वजनिक ब्लॉक पूरे लेन-देन लॉग को नेटवर्क

पर सभी कंप्यूटरों पर दोहराते हैं, उपयोग के दौरान हिरासत की श्रृंखला को प्रतिबंधित करना असंभव है। इस प्रकार, ब्लॉक श्रृंखला प्रौद्योगिकी के लिए "लेखक पुस्तक" दृष्टिकोण का जन्म हुआ। ब्लॉक जोड़ने वाले लोगों की पहचान एक अनुमत खाता बही में जानी जाती है, और सिस्टम में डेटा केवल चयनित पार्टियों द्वारा ही देखा जा सकता है। क्योंकि लॉटरी के आधार पर कोड चलाने वाले लोगों द्वारा नए ब्लॉक बनाने का अधिकार सौंपा गया है, इसके लिए भुगतान करने के लिए प्रूफ-ऑफ-वर्क माइनिंग या क्रिप्टो रूपांतरण करने की कोई आवश्यकता नहीं है। इस प्रकार की प्रणाली का उपयोग उन स्थितियों में किया जाना है जहां ब्लॉक श्रृंखला में सभी प्रतिभागियों को पहले से ही एक-दूसरे पर कुछ भरोसा है, लेकिन बैंकों के मामले में एक तटस्थ तृतीय पक्ष की सेवाओं का अनुकरण करना चाहते हैं। अंतरराष्ट्रीय स्थानान्तरण कर सकता है। पिछले साल, R3 - जिसने हाल ही में 40 संस्थानों से $107 मिलियन जुटाए - ने अपना पहला अधिकृत ऑर्डर बुक लॉन्च किया: कॉर्डा। और कॉर्डा के पास पहले से ही एक प्रतियोगी है: जेपी मॉर्गन, जिन्होंने पिछले वसंत में आर 3 कंसोर्टियम को कोरम नामक अपना स्वयं का लाइसेंस प्राप्त बहीखाता लॉन्च करने के लिए छोड़ दिया।

निष्कर्ष

मोनास इंडस्ट्रीज के सह-संस्थापक प्रेस्टन बर्न कहते हैं, ब्लॉक चेन डेवलपर्स के लिए एक खुला मंच, वे मानक वित्तीय सेवाओं और सरकार समर्थित मुद्राओं में जाते हैं। "इसलिए जब पैसा उनके रास्ते में बहना शुरू हो जाता है, तो वे जनता के लिए उतने ही बेखबर होते जा रहे हैं - जिनका वे कभी हिस्सा थे।" दूसरी ओर, एप्लिकेशन-विशिष्ट मुद्रा केवल एक वित्तीय साधन नहीं है, बल्कि एक तकनीक है। पहुँचनेका जरिया। जितने अधिक लोग प्रौद्योगिकी सेवा का उपयोग करते हैं, उस सेवा तक पहुँचनेके लिए जारी की गई मुद्रा की माँग उतनी ही अधिक होती है। समय बदल गया है, और बहुत जल्दी। लेवी डी हरारे कहते हैं, कुछ शुरुआती दत्तक ग्रहण करने वाले, जो तीन और चार साल पहले आर्थिक रूप से बाहर थे, अभी भी अपनी मान्यताओं और अपनी मुद्राओं पर कायम हैं, अब बहुत अच्छा कर रहे हैं।



ग्रन्थ सूची

एडमिनिस्ट्रेशन फ़ेडरल डे इंग्रेस पब्लिक (2019), रेज़ोल्यूशन 4614/2019 - इन्फो लेग, (2 अक्टूबर 2020 को देखा गया) ।

प्रत्यक्ष योगदान का प्रशासन, लक्ज़मबर्ग (2018), योगदान निदेशक का परिपत्र (27 जुलाई 2020 को देखा गया) ।

Agenize Entreat, इतालवी अर्थव्यवस्था और वित्त मंत्रालय (2016), संकल्प N.72, 27 जुलाई 2020 को एक्सेस किया गया) ।

बैंको सेंट्रल डे ला रिपब्लिकन डोमिनिकन (2017), कम्युनिकेटर,(29 जुलाई 2020 को एक्सेस किया गया)।

बैंको सेंट्रल डेल इक्वाडोर (2018), कम्युनिकेटर ऑफिशियल सोबर एल यूज डेल बिटकॉइन, (29 जुलाई 2020 को एक्सेस किया गया)।

संघीय कर प्रशासन, स्विट्जरलैंड (2019), क्रिप्टोकरेंसी (27 जुलाई 2020 को देखा गया) ।

कनाडा राजस्व एजेंसी (2019), क्रिप्टोक्यूरेंसी और कर पेशेवरों के उपयोगकर्ताओं के लिए आभासी मुद्रा के लिए गाइड, (27 जुलाई 2020 को एक्सेस किया गया) ।

ईसीबी क्रिप्टो-एसेट्स टास्क फोर्स (2019), क्रिप्टो-एसेट्स: वित्तीय स्थिरता, मौद्रिक नीति और भुगतान और बाजार बुनियादी ढांचे के लिए निहितार्थ, http://dx.doi.org/10.2866/162।

पेरिस-ला डिफेंस स्कूल ऑफ इंजीनियरिंग ESILV (2019) फ्रांस में क्रिप्टोकरेंसी और कर: सभी (27 जुलाई 2020 को देखा गया) ।