Freeman Family

जुलाई 4,2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

EPIC

सहकर्मी-से-सहकर्मी वाली इलेक्ट्रॉनिक नकद व्यवस्था

स्टोर ऑफ़ वैल्यू (मूल्य संचय) + आदान-प्रदान का साधन + लेखा इकाई (यूनिट ऑफ़ अकाउंट)

1.7 बिलियन लोग ऐसे हैं जिनके पास वैश्विक फाइनेंसियल साधनों तक पहुंच नहीं है, जबकि **1.3** बिलियन ऐसे लोग हैं जो ऐसी सेवा से वंचित हैं। व्यक्तियों को वैश्विक बाजार तक पहुँच प्रदान करके **Epic Cash** इस सुविधा को उपलब्ध कराता है। तेज़, वर्चुअल रूप से मुफ्त उपयोग, और सभी के लिए उपलब्ध।

Version 7.1b Hindi

अंतर्वस्तु

I. संक्षिप्त विवरण

Epic Cash, *वास्तविक* P2P *इंटरनेट नकद के मार्ग में आखरी मंजिल है, एक निजी फाइनेंसियल व्यवस्था का आधार।* Epic *मुद्रा डिजिटल धन के रूप का दुनिया का सबसे प्रभावी प्राइवेसी-सुरक्षित रूप बनना चाहता है। इस लक्ष्य को हासिल करने के लिए, यह धन के तीन प्रमुख कार्यों को पूरा करता है:*

1. **मूल्य संचय -** बाद में इसे बचाया जा सकता है, फिर से प्राप्त किया जा सकता है और एक्सचेंज किया जा सकता है, और फिर से प्राप्त किए जाने पर यह अनुमानित कीमत की होगी;
2. **आदान-प्रदान का साधन** – किसी मानक मूल्य को रेप्रेसेंट करने वाले जैसा और वस्तुओं या सेवाओं के लिए जो एक्सचेंज किया जा सके वह स्वीकार्य है;
3. **लेखा इकाई -** वह इकाई जिसकी मदद से किसी वस्तु के मूल्य को निर्धारित किया जा सकता है और उसकी तुलना की जा सकती है।

	$ USD	BTC	EPIC
मूल्य संचय	✗	✓	✓
आदान-प्रदान का साधन	✓	✗	✓
लेखा इकाई	✓	✗	✓

2009 में, बिटकॉइन एक सर्वप्रथम ब्लॉकचेन-आधारित डिजिटल मुद्रा के रूप में विकसित हुई**,** और इसके साथ तीन ऐसी विशेषताएं हैं जिनके साथ अन्य क्रिप्टोमुद्राओं का मूल्य निर्धारित किया जाता है:

- ट्रस्टलिसनिस – नेटवर्क के संचालन के लिए किसी भी तत्व को किसी सेंट्रलाइज्ड इकाई या प्रतिपक्ष पर भरोसा करने की आवश्यकता नहीं है**;**
- अपरिवर्तनीयता (जिसे बदला नहीं जा सकता) – किये गए सौदे वापस बदले नहीं जा सकते**;**
  इसे फिर से दोहराना अत्यधिक असंभव या मुश्किल होना चाहिए**;**
  सिवाय प्राइवेट की के मालिक के किसी अन्य व्यक्ति के लिए उस प्राइवेट की से जुड़े धन का इस्तेमाल करना असंभव होना चाहिए**;**
  सारे सौदे ब्लॉकचेन पर दर्ज किए जाते हैं।
- ड सेंट्रलिज़ेशन - "ब्लॉकचेन राजनीतिक रूप से ड सेंट्रलाइज्ड (अनियंत्रित) होते हैं (उन्हें कोई भी नियंत्रित नह कर सकता है) और आर्किटेक्चरल रूप से ड सेंट्रलाइज्ड होते हैं (असफलता का कोई आधार नह है) ..."।[1]

बिटकॉइन ने अपनी मोनेटरी नीति के मुताबिक समयसिद्ध मौलिक तत्वों का पालन करके तकनीकी रूप से नए रूप सामने लाये हैं। बिटकॉइन की सफलता उसकी सीमित सप्लाई के साथ ट्रस्टलिस, अपरिवर्तनीय और डीसेंट्रलाइज्ड ब्लॉकचेन से जुड़ा है। Epic Cash बिटकॉइन की कम इन्फ्लेशन वाली मोनेटरी नीति का इस्तेमाल करता है ताकि वह यह सुनिश्चित कर सके कि Epic मुद्रा एक प्रभावी मूल्य संचय के रूप में काम कर सकता है।

बिटकॉइन की सफलता के बावजूद, 10 साल पहले इसकी शुरुआत से कुछ कमियां सामने आई हैं। अन्य प्रोजेक्ट ने इन कमियों को हल करने की कोशिश की और हमने अपने शुरुआती समय में इनमें से सबसे सफल प्रोजेक्ट की जांच की है जिसे हम उदाहरण के रूप में इस्तेमाल कर सकते हैं। हमने Grin कोडबेस का और बहुत सारे अन्य प्रोजेक्ट के बेहतरीन काम का इस्तेमाल करना तय किया है ताकि हम कड़ी मेहनत से जीती सफलताओं पर निर्णय ले सकें और इस तरह हम Epic Cash के पहले आए प्रोजेक्ट की खामियों का पता लगा पाएं। Epic Cash में एक आदर्श मुद्रा बनने के मुख्य गुण हैं:

- फंगिबिलिटी– किसी एक **Epic** के यूनिट का मूल्य हमेशा दूसरों **Epic** यूनिट के बराबर होना चाहिए**,** जिस तरह एक **Yen** या **Yuan** हमेशा दूसरे **Yen** या **Yuan** के बराबर होता है और बदली किया जा सकता है। फंगिबिलिटी की सफलता काफी हद तक प्राइवेसी पर टिकी है।
- **स्केलेबिलिटी** - **Epic Cash** के पास एक ऐसा कुशल ब्लॉकचेन है**,** जिस पर रिसोर्स से भरे उपकरण के बिना नए नोड आसानी से स्थापित किए जा सकते हैं। **Epic Cash** ब्लॉकचेन बिटकॉइन के कम से कम दुगने थ्रुपुट (प्रवाह क्षमता) की क्षमता रखता है।
- प्राइवेसी - **Epic Cash** ब्लॉकचेन बाहरी दलों से सौदों का विवरण छुपाकर **Epic** धारकों और उपयोगकर्ताओं के डिटेल्स की रक्षा करता है**,** और यह निगरानी से दूर और अदृश्य है।
- गति - **Epic Cash** के सौदे सरल**,** निरंतर होते हैं और उन्हें ब्लॉकचेन तकनीक के पिछले तकनीकों के मुकाबले और तेज़ी से पूरा किया जाता है। जहाँ एक तरफ बिटकॉइन को सौदे की पुष्टि के लिए छह **10-**मिनट के ब्लॉकों की आवश्यकता होती है**,** वहां दूसरी तरफ जैसे ही **1-**मिनट के ब्लॉक माइन किए जाते हैं वैसे ही एक एकल सौदे की पुष्टि के अंदर-अंदर **Epic** के सौदे होते हैं।

[1] **Buterin, Vitalik,** *The Meaning of Decentralization*, **6 February, 2017,** https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. पराइवेसी

पैसे का आधुनिक प्रयोग का मतलब है लोगों और संस्थानों के बीच लेखा इकाइयों का कलेक्टिव ट्रान्सफर। किसी भी वक्त पैसे का पूरा नज़ारा नीचे दिए गए सवालों का जवाब देकर समझा जा सकता है:

1. *इसे होल्ड कौन कर रहा है, और वे कितना होल्ड कर रहे हैं?*
2. *कौन किसके साथ और कितने के लिए सौदा कर रहा है?*

पारंपरिक फिएट मुद्राओं और असल में बिटकॉइन के लिए भी, हम इन सवालों के जवाब दे सकते हैं। ऐसा करके, लोगों के जीवन के बारे में काफी कुछ पता लगाया जा सकता है, जैसे इस्तेमाल के पैटर्न, ओनरशिप और सौदों के प्रतिपक्ष। कितने मूल्य का ट्रान्सफर किया गया है यह पता लगाकर किसी व्यक्ति की रुचियों और इरादों का पता लग सकता है। प्राइवेसी के बिना, अगर यह जानकारी बुरे बाहरी दलों के हाथ लग जाती है तो यह लेनदेन डेटा खतरनाक जानकारी हो सकती है।

क्रिप्टोमुद्रा के पिछले एक दशक के प्रयोग से अलग-अलग ब्लॉकचेन के इम्प्लीमेंटेशन में "प्राइवेसी" की एक निरंतरता पता चलती है। प्राइवेसी का पैमाना, अगर इसपर विचार किया जाता है, एक ओर से खुला और लोकप्रिय और दूसरी ओर से अज्ञात है। जैसे-जैसे प्राइवेसी खत्म हो जाती है, क्रिप्टोमुद्रा का एक जरूरी आधार, ट्रस्टलिसनिस कम हो जाता है। जैसे कि बिटकॉइन ब्लॉकचेन एनालिसिस सेवाओं की सफलता में देखा गया है, बिटकॉइन प्राइवेसी के मामले में खुले तौर पर ट्रांसपेरेंट है। उपयोगकर्ताओं को ध्यान में रखना चाहिए कि वे अविश्वसनीय बिटकॉइन में अनजाने से सौदा न करें। **Epic Cash** का समाधान काफी हद तक अज्ञात है और वह इस महत्वपूर्ण गुण को फिर से प्राप्त करता है जिसके लिए वह सुनिश्चित करता है कि व्यक्ति की प्राइवेसी और सौदों की प्राइवेसी मौलिक तौर पर व्यवस्था में शामिल हैं।

पहचान की प्राइवेसी

सौदों की प्राइवेसी

पहचान की प्राइवेसी

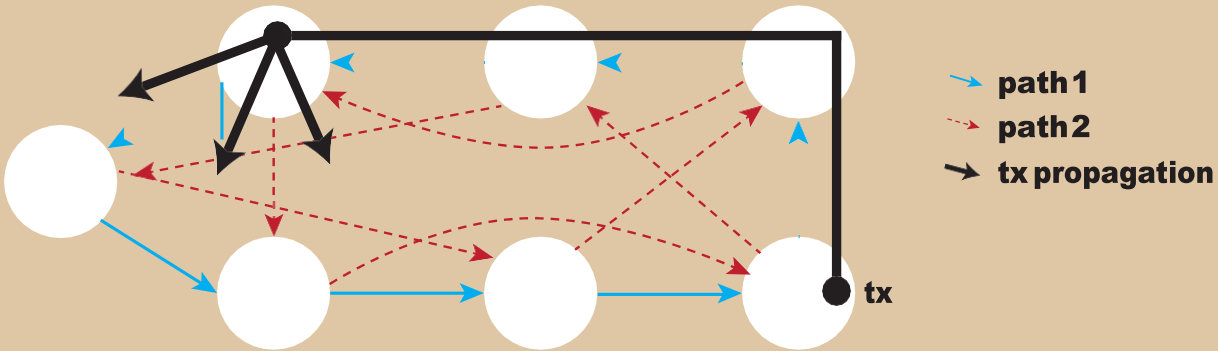
बिटकॉइन जैसी अधिकतर क्रिप्टोमुद्राएं ऐसे वॉलेट में स्टोर किए जाते हैं जिनके पते किसी वॉलेट की प्राइवेट की से प्राप्त पब्लिक चाबी से जुड़े हैं। डिजिटल दुनिया में हम इन पतों को किसी के प्राइवेट वॉल्ट के लोकेटर जैसा मान सकते हैं। Epic Cash ब्लॉकचेन पते की परिभाषा पूरी तरह से मिटाता है और इसके बदले एक बड़ा बहु-हस्ताक्षर लागू करता है जिससे एक टाइम के उपयोग के लिए सभी सार्वजनिक और प्राइवेट चाबियों को उत्पन्न किया जा सकता है।

क्योंकि डिजिटल दुनिया में बिटकॉइन वॉलेट पते किसी वॉल्ट के लोकेटर होते हैं, इसलिए उस वॉलेट से किसी मालिक के इंटरनेट प्रोटोकॉल **(IP)** पते का पता लगाया जा सकता है, जिससे फिर किसी निश्चित समय पर एक अनोखे स्थान पर किसी कंप्यूटर के मालिक का पता चलता है। सरल रूप से समझाए तो: जब बिटकॉइन का सौदा होता है, तब सौदा 'नोड' नामक एक संचार केंद्र से प्रसारित किया जाता है और फिर 'पीयर्स' नामक अन्य नोडों तक प्रसारित किया जाता है। यह जानकारी फिर पूरे नेटवर्क में लगातार हर एक नोडों के पीयरों तक फैलती है। इस प्रक्रिया को "गॉसिप प्रोटोकॉल" का सही नाम दिया गया है। मतलब, हर एक बिटकॉइन की एक ऑनलाइन स्थिति होती है और एक फिजिकल स्थान होता है जिसे देखा जा सकता है, जहां वह या फिर कहे, बिटकॉइन का मालिक पाया जा सकता है। जैसे कि पत्रकार **Grace Caffyn** ने कहा, बिटकॉइन "उतना ही गुप्त है जितना घर के इंटरनेट कनेक्शन से **Google** पर किया गया खोज।"[2]

वॉलेट पते की जरूरत मिटाने के साथ, **IP** पतों के ट्रेस होने की संभावना मिटाकर, **Epic Cash** ब्लॉकचेन पहचान की प्राइवेसी को सुरक्षित करता है। इसके लिए वह ***Dandelion ++*** प्रोटोकॉल का इस्तेमाल करता है। अपने से पहले आये प्रोटोकॉल (मूल ***Dandelion*** प्रोटोकॉल) का बेहतर रूप, ***Dandelion ++*** प्रोटोकॉल ब्लॉकचेन पर डी-ऐननिमिज़ेशन (डेटा की प्राइवेसी मिटाने) के हमलों का सामना करने के लिए बनाया गया ऐसा प्रोटोकॉल है जो सात शोधकर्ताओं की कड़ी-मेहनत का फल है। ***Dandelion ++*** के जरिए, सौदे रैंडम एक-साथ जुड़े रास्तों या, 'केबलों' से गुज़रते हैं, और फिर नोडों के एक बड़े नेटवर्क में अचानक फैल जाते हैं, वैसे ही जैसे ***Dandelion*** फूल की फली जब अपने स्टेम से निकाली जाती है (चित्र **1**)। इससे सौदों के ओरिजिन का पता लगाना लगभग असंभव हो जाता है, और इस तरह उनके मूल **IP** पतों का पता लगाना भी।

चित्र 1: Dandelion ++ प्रोटोकॉल के साथ सौदों को अज्ञात बनाना।

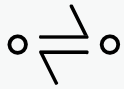
Dandelion ++ एक **4**-रेगुलर ग्राफ़ पर दो एक-साथ जुड़े रास्तों में से एक पर संदेश भेजता है, फिर प्रसार प्रक्रिया का इस्तेमाल करके उन्हें फैलाता है। चित्र में, सौदा नीले रास्ते से फैलता है।[3] इस प्रक्रिया से सौदों के ओरिजिन का पता लगाना एकदम मुश्किल बन जाता है, जिससे प्राइवेसी सुरक्षित की जाती है।



[2] **F2Caffyn, Grace,** *Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,* **14 March, 2015,** https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] **Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees',** *Proc. ACM Meas. Anal. Comput. Sys.,* **Vol. 2, Article 29, pg. 8,** https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

सौदे की प्राइवेसी



Epic Cash ब्लॉकचेन सौदों की राशियों और भेजने-प्राप्त करने वाले के बीच के संबंध को अस्पष्ट करके सौदे की प्राइवेसी को सुरक्षित करता है। यह Gregory Maxwell (बिटकॉइन कोर विकासक, Blockstream के सह-संस्थापक और CTO) द्वारा विकसित *गोपनीय सौदे* (CT)[4] और *CoinJoin*[5] तरीकों को लागू करके हासिल किया जाता है।

CT, Adam Back द्वारा मूल रूप से बनाया गया और फिर **Maxwell** द्वारा तराशा गया, होमोमोर्फिक एन्क्रिप्शन (प्राइवेसी संरक्षित करने के लिए एन्क्रिप्टेड जानकारी पर, उसे डिक्रिप्ट किए बिना, गणना करने का एक तरीका) के जरिए सौदों को छोटे भागों में विभाजित किया जाता है। विभाजित होने के बाद, दर्शक ब्लाइंडिंग (अदृश्य करने वाले) कारकों के कारण सौदों की वास्तविक राशि नहीं देख सकते हैं, एक ऐसी व्यवस्था जो सौदों के भागों के मिश्रण में रैंडम अंक डालती है ताकि उन भागों के मूल्यों को छिपाया जा सके। आखिरकार, सिर्फ सौदा करने वाले दलों को एक्सचेंज की राशि का पता होता है, जिसके दौरान सौदे की पुष्टि नेटवर्क करती है जिसके लिए वह यह पुष्ट करती है कि क्या इनपुट वैल्यू का जोड़ आउटपुट वैल्यू के जोड़ के बराबर है और इनपुट ब्लाइंडिंग कारकों का जोड़ आउटपुट ब्लाइंडिंग कारकों के बराबर है।

ताक-झाँक करने वालों के कार्य को और मुश्किल बनाने के लिए, सभी **Epic Cash** सौदों को **CT** के साथ जोड़ा जाता है और फिर सौदा करने वाले दलों के बीच कनेक्शन को छिपाने के लिए एक साथ मिलाया जाता है। यह **Maxwell** की दूसरी धारणा, **CoinJoin** की मदद से किया जाता है।

CoinJoin को सरल रूप से मझाने के लिए, सोचें कि **A, B** और **C X, Y** और **Z** को **Epic** भेज रहे हैं। **CoinJoin** साधन की मदद से सौदा भेजकर, सिर्फ यह पता चलता है कि **A, B** और **C** भेज रहे हैं और **X, Y** और **Z** प्राप्त कर रहे हैं, जबकि सौदों की राशि अदृश्य रहती है। वन-वे एग्रीगेट सिग्नेचर (**OWAS**) के जरिए **CoinJoin** व्यवस्था **Epic Cash** के लिए मौलिक है, जिसमें एक ब्लॉक में मौजूद सभी सौदों को एक ही सौदे में जोडा जाता है।

प्राइवेसी: सारांश (समरी)

Epic Cash ब्लॉकचेन इन तरीकों का पालन करके व्यक्तियों और उनके सौदों की प्राइवेसी की रक्षा करता है:

- वॉलेट पते की जरूरत मिटाकर - ब्लॉकचेन में डिजिटल वाल्टों से जुड़ा कोई स्थान पहचानकर्ता उपलब्ध नहीं है। सौदे एक वॉलेट-से-वॉलेट आधार पर सीधे तौर पर व्यक्ति-से-व्यक्ति तक बनाए जाते हैं;
- *कॉंफिडेंशल सौदे* – सौदों को कई भागों में विभाजित करना और ब्लाइंडिंग कारकों को उन भागों के कलेक्शन में इस्तेमाल करना, ताकि उन भागों का मूल्य और अन्य लेनदेन कारकों के बारे में कोई नहीं जान पाए;
- ***Dandelion++*** प्रोटोकॉल – सौदा भेजने वाले के **IP** पते से किसी सौदे के डिजिटल मार्ग को छिपाता है;
- ***CoinJoin*** – सौदा करने वाले दलों के बीच संबंधों को छिपाने के लिए सौदों को बंडलों में कलेक्ट करता है।

[4] **Maxwell, Gregory,** *Confidential Transactions,* **Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt**

[5] **Maxwell, Gregory,** *CoinJoin: Bitcoin Privacy for the Real World*, **22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0**

III. फंगिबिलिट

लाइटकॉइन के निर्माता **Charlie Lee** ने कहा कि बिटकॉइन और लाइटकॉइन से वास्तविक धन का केवल एक गुण मिस्सिंग है और वह है फंगिबिलिटी, जिससे यह स्पष्ट हो जाता है कि ये सिक्के प्राइवेसी और फंगिबिलिटी पर काम करने वाले हैं।[6] **Andreas Antonopoulos** जो दुनिया के सबसे बड़े ब्लॉकचेन एक्सपर्ट में से एक हैं, उन्होंने दावा किया कि **"...** अविश्वसनीय सिक्के खतरनाक हैं।**"** अगर आप फंगिबिलिटी और प्राइवेसी को नुकसान पहुंचाते हैं, तो आप मुद्रा को नुकसान पहुंचाते हैं।"[7]

फंगिबिलिटी वस्तुओं या संपत्ति के एक सेट का ऐसा गुण है जो सुनिश्चित करती है कि उस सेट के व्यक्तिगत यूनिट समान मूल्य के हैं और उनका एक्सचेंज किया जा सकता है। यह एक ऐसा गुण है जो मुद्रा के सबसे पुराने रूपों को पहले की आदान-प्रदान वाली पुरानी व्यवस्थाओं से अलग करती है। पैसे की फंगिबिलिटी पर भरोसा करे बिना, वह पैसा तेजी से अपनी उपयोगिता खोती है। जैसा कि नीचे दर्शाया गया है, अधिकतर क्रिप्टोमुद्राओं की फंगिबिलिटी अनिश्चित है, जबकि **Epic Cash** की प्राइवेसी संरचना सुनिश्चित करती है कि यह समान खतरों को रोक सकती है।

बिटकॉइन के समान अधिकतर क्रिप्टोमुद्राएं, उस ट्रांसपेरेंट ब्लॉकचेन के रूप की तरह जिस पर वे मौजूद हैं, हर उस वॉलेट की मदद से ट्रेस की जा सकती हैं जिसमें उन्हें रखा गया था। समान रूप से निजी बाहरी दल और सरकार पिछली गतिविधियों में इस्तेमाल किए गए सिक्कों की तत्काल पहचान करने के लिए और मुश्किल तरीकों से बिटकॉइन ब्लॉकचेन की निगरानी करते हैं। स्वाभाविक तौर पर हमें यह चिंता होती है कि किसी दिन अविश्वसनीय सिक्कों को सौदों से प्रतिबंधित किया जाएगा जिससे उनके मासूम धारकों को नुकसान हो सकता है।

19 मार्च, **2018** को, **U.S.** के विदेश संपत्ति संचालन (**OFAC**) ने घोषणा की कि वह डिजिटल मुद्रा पतों को खास तौर से नामित नागरिकों (**SDN**) की सूची में शामिल करने पर विचार कर रहा है, जो ऐसे इकाई हैं जिनके साथ **U.S.** व्यक्तियों या कारोबारों को सौदा करने पर पाबंदी लगाई गई है।

इससे ज्यादा परेशानी की बात यह है कि **OFAC** ने **SDN** सूची में अविश्वसनीय सिक्कों को रखने वाले पतों को शामिल करने से भी इनकार नहीं किया है, जिससे अविश्वसनीय सिक्कों के मासूम मालिकों को प्रभावी रूप से एक आपराधिक ब्लैकलिस्ट में शामिल किया जाएगा क्यूंकि वे अविश्वसनीय क्रिप्टोमुद्राओं से संबंध रखते हैं। इसके कारण न्यूयॉर्क यूनिवर्सिटी के कानूनी प्रोफेसर, **Andrew Hinkes** ने ताना मारते हुए कहा **"**फंगिबिलिटी को प्रेम से अलविदा कहने का वक्त आ गया है" और अब "अभी—अभी बनाए गए सिक्कों, या ट्रेस किए गए साफ़ सिक्कों पर एक प्रीमियम..." लगाए जाने की उम्मीद करनी चाहिए जनता को।[8]

इन नई बातों को ध्यान में रखते हुए, क्रिप्टो बाजार में उथल-पुथल की कल्पना करना और कई सफल क्रिप्टोमुद्राओं की कठिनाई या यहां तक कि समाप्ति की कल्पना करना दूर नहीं है। हालांकि, **Epic** उन कुछ गिने-चुने क्रिप्टोमुद्राओं में से एक है जो इस समस्या को पूरी तरह हल करती है क्योंकि उसके पास इस दस्तावेज़ में बताई गई मजबूत प्राइवेसी विशेषताएं उपलब्ध हैं। पहचान और ओनरशिप के बीच की कड़ी मिटाकर, और लेन-देन करने वाले दलों के बीच संबंध मिटाकर, **Epic** को कभी भी किसी व्यक्ति या गतिविधि से जोड़ा नहीं जा सकता है। अभी तक, **Epic** का मूल्य उसके उपयोगकर्ताओं पर निर्भर नहीं है और वह प्राइवेसी और सुरक्षा के उच्च स्तर प्रदान करता है जिन्हें आपराधिक, फाइनेंसियल या राजनीतिक क्षेत्र में बुरे कारकों द्वारा आसानी से बदला नहीं जा सकता है।

> “... अविश्वसनीय सिक्के खतरनाक हैं।" अगर आप फंगिबिलिटी और प्राइवेसी को नुकसान पहुंचाते हैं, तो आप मुद्रा को नुकसान पहुंचाते हैं।”
>
> ANDREAS ANTONOPOULOS

[6] **Njui, John P,** *Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility*, **29 January, 2019,** https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] **Carl T,** *Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,* **9 April, 2019,** https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] **Hinkes, Andrew, Ciccolo, Joe,** *OFAC's Crypto Blacklist Could Change Crypto*, **24 March, 2018,** https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. सकालाबिलिटि

Epic Cash एक **MimbleWimble** ब्लॉकचेन इम्प्लीमेंटेशन है जो स्कालाबिलिटी के मामले को हल करता है क्योंकि उसके पास स्पेस कुशल डिजाईन है जो अनावश्यक लेनदेन के डेटा को नष्ट करता है। इसके लिए जिम्मेदार कट-थ्रू फंक्शनलिटी सुनिश्चित करती है कि ब्लॉकचेन, बिटकॉइन सहित अन्य क्रिप्टोमुद्राओं से अलग, समय के साथ अधिक स्पेस कुशल बन सके और कि मेमोरी और कंप्यूटिंग पॉवर में कम से कम निवेश करके नए नोड बनाए जा सके। स्पेस कुशल रहकर, यह व्यापक रूप से फैले नेटवर्क को शामिल करता है और डीसेंट्रलिज़ेशन को बढ़ावा देता है। इसके अलावा, जहाँ एक तरफ हर एक बिटकॉइन नोड को पूरी चेन स्टोर करना पड़ता है, ब्लॉकों के एक छोटे से विभाजित भाग के आधार पर **Epic Cash** के नोड नेटवर्क सुरक्षा में मदद कर सकते हैं।

अधिकतर क्रिप्टोमुद्राओं को अपने ब्लॉकचेन पर सारे लेनदेन डेटा को स्टोर करने के लिए अनगिनत स्टोरेज की जरूरत पड़ती है। फिलहाल बिटकॉइन चेन हर दिन **0.1353 GB** की मेमोरी प्राप्त करती है, और दूसरी तरफ इथेरियम की चेन हर दिन **0.2719 GB** की मेमोरी प्राप्त करती है। अगर बिटकॉइन की चेन इस दर से बढ़ती रहेगी, तो यह **2140** तक साइज़ में लगभग **6 TB** का हो जाएगा जब इसका अंतिम इनाम ब्लॉक माइन किया जाएगा। इथेरियम उस तारीख तक **10 TB** पार कर लेगा।[9] **MimbleWimble** के बिना अधिकतर ब्लॉकचेन में, सौदे दुनिया भर के नोडों द्वारा पुष्ट होते हैं। जैसा-जैसा डेटा बढ़ता है, हर नोड पर बोझ भी बढ़ता है। यहां तक कि सिर्फ **200 GB** (मौजूदा बिटकॉइन चेन का अनुमानित साइज़) के साथ, डेटा को सिंक्रनाइज़ करने के लिए एक स्टेबल नेटवर्क और उच्च गति डिस्क रीड और राईट की क्षमता जरूरी है।

नतीजतन, महंगे कंप्यूटिंग रिसोर्सेज का इस्तेमाल करके माइनिंग बड़े पूलों के बीच तेजी से सेंट्रलाइज्ड हो रहा है। अगर **Epic Cash** के ब्लॉकचेन पर बिटकॉइन के पूरे ब्लॉकचेन इतिहास को स्टोर किया जाता तो यह लगभग **90%** तक कम जगह में फिट हो जाता। छोटी जगह से गति बढती है क्योंकि हर लेनदेन को प्रसारित होने और सुरक्षित रखने में कम समय लगता है।

MimbleWimble, ब्लॉक प्रूनिंग की एक नई सोच वाले विचार के साथ इस स्टोरेज की दुविधा को हल करता है, जिसे 'कट-थ्रू' नाम दिया गया है। कट-थ्रू कैसे काम करता है, यह समझने के लिए, सबसे पहले यह देखना जरूरी है कि किसी **MimbleWimble** ब्लॉकचेन में सौदे और ब्लॉक कैसे बनाए जाते हैं।

इनपुट:

पुराने आउटपुट के रिफरेन्स;

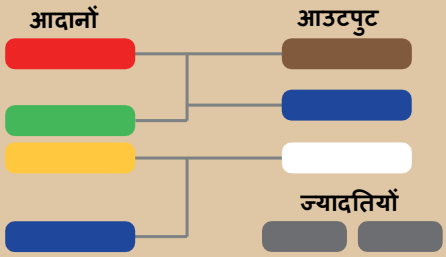
आउटपुट:

कांफिडेंशियल सौदों के आउटपुट और रेंजप्रूफ;

अतिरिक्त:

आउटपुट और इनपुट के बीच का अंतर और उसके साथ हस्ताक्षर भी (ऑथेंटिकेशन के लिए और गैर-इन्फ्लेशन साबित करने के लिए)।

चित्र 2:
MimbleWimble सौदों के भाग।



[9] **Li, Crypto,** *Blockchain's Big Data Problem,* **27 January, 2019,** https://www.longhash.com/news/blockchains-big-data-problem

सारे **Epic Cash** ब्लॉकों में ये शामिल हैं:

लेनदेन इनपुट के मर्कल ट्रीज;

लेनदेन आउटपुट और रेंजप्रूफ के मर्कल ट्रीज;

अतिरिक्त मूल्यों और हस्ताक्षरों की एक सूची।

Andrew Poelstra की प्रस्तुतियों से प्रेरित चित्र **2** और **3** में[10], हम देख सकते हैं कि नए बनाए गए **Epic** को सफेद इनपुट सेलों के रूप में दर्शाया गया है। समान रूप से रंगीन सेल खर्च किए गए इनपुट से संबंधित आउटपुट को दर्शाते हैं। कट-थ्रू प्रक्रिया के साथ, इनपुट और उनसे संबंधित आउटपुट को निकाला जाता है ताकि ब्लॉक में जगह बनाया जा सके, जिससे ब्लॉकचेन पर स्टोर किए जाने वाले डेटा का वॉल्यूम कम हो जाती है। जहाँ एक तरफ लेनदेन लेजर में शामिल नहीं किए जाते हैं, दूसरी तरफ बाकी बचे अतिरिक्त कर्नेल (मात्र **100** बाइट के) स्थायी रूप से यह जानकारी दर्ज करते हैं कि सौदे हुए हैं।

जैसे-जैसे ब्लॉक बनाए जाते हैं, **MimbleWimble** ब्लॉकों पर कट-थ्रू लागू कर देता है, ताकि आगे चलकर सिर्फ ब्लॉक हेडर (लगभग **250** बाइट), बाकी बचे सौदे और लेन-देन तत्व (लगभग **100** बाइट) बचते हैं। **Grin,** जो लॉन्च किए जाने वाला दूसरा **MimbleWimble** इम्प्लीमेंटेशन है, ने दिखाया कि बिटकॉइन चेन के समान संख्या के सौदों वाला एक **MimbleWimble** चेन बिटकॉइन की चेन के साइज़ का लगभग **10%** हिस्सा होगा।[11] इसके अलावा, नोड का साइज़ "किसी बिटकॉइन-साइज़ वाले चेन के मुताबिक कुछ **GB** का, और संभव रूप से कुछ सौ मेगाबाइट तक ऑप्टिमाइज़ करने योग्य" होगा।[12]

यह बिटकॉइन से अलग है, जहां हर एक ब्लॉकचेन को हर एक नोड द्वारा स्टोर किया जाना चाहिए। समय के साथ, जैसे-जैसे **Epic Cash** ब्लॉकचेन की स्पेस कुशलता बिटकॉइन ब्लॉकचेन के जैसे बढ़ती है, उसी तरह **Epic Cash** नेटवर्क में नोडों की भागीदारी से संबंधित लागत क्षमताएं भी बढेंगी। भाग लेने में कम बाधाएँ होने से नेटवर्क डिज़ाइन के नोड स्तर पर मुश्किलें रोकने की महत्वपूर्ण क्षमता प्राप्त होती है।

MimbleWimble के इसके इम्प्लीमेंटेशन और कट-थ्रू प्रक्रिया के साथ चेन प्रूनिंग के इस्तेमाल से, **Epic Cash** ब्लॉकचेन एक तरह से स्केलेबिलिटी पेश करता है जिसे अक्सर क्रिप्टोमुद्रा समुदाय अनदेखा कर देता है। यह बिटकॉइन और समान प्रोजेक्ट की धारणा का पालन करता है: डीसेंट्रलिज़ेशन। इसपर ध्यान दिए बिना कि कोई सिक्का हर सेकंड कितने सौदे प्रोसेस कर सकता है, उसका क्या फायदा है अगर उसे कोई व्यापक और डाइवर्स नेटवर्क संभाल ही नहीं सकता है? अगर मेमोरी की जरूरतें ऐसी हैं, कि वेलिडेशन के लिए अंत में मजबूत माइनिंग समूहों के पास जाना पड़े, तो एक डीसेंट्रलाइज्ड व्यवस्था बनाने के क्रिप्टोमुद्रा समुदाय के सभी प्रयासों का कोई फायदा नहीं। अतिरिक्त थ्रूपुट प्रदान करने के लिए, **Epic Cash** के विकास सूची में लाइटनिंग-स्टाइल लेयर **2** के इम्प्लीमेंटेशन को एक छोटे समय के उद्देश्य के रूप में शामिल किया गया है।

चित्र 3: **MimbleWimble** सौदे कट-थ्रू से पहले और बाद में।

[10] **SF Bitcoin Developers,** *MimbleWimble with Andrew Poelstra,* **24 November, 2016,** https://www.youtube.com/watch?v=aHTRIbCaUyM&t=940s

[11] **Grin Forum,** *Grin Blockchain Size,* **December, 2018,** https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] **GandalfThePink,** *Introduction to Mimblewimble and Grin,* **28 March, 2019,** https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. मोनेटरी नीति

Epic Cash और बिटकॉइन की मोनेटरी नीति काफी एक-जैसी है। Epic Cash की चल (सर्क्युलेटिंग) सप्लाई पहले तो तेजी से फैलती है और फिर 2028 में बिटकॉइन की चल सप्लाई के साथ सिंक में होती है। यह फिर एक घटती दर पर बढ़ती है जब तक वह 2140 में 21 मिलियन की अधिकतम सप्लाई तक नहीं पहुँच जाती। Epic Cash के पास क्षमता है कि वह दीर्घावधि (लंबे समय तक) मूल्य का सुरक्षित भंडार बन सके क्यूंकि उसके एमिशन जीवनचक्र के दौरान हर वक्त उसकी चल सप्लाई का पता सबको है और वह एक निश्चित अधिकतम सप्लाई में समाप्त हो जाती है। Epic Cash की मोनेटरी नीति इन चार विशेषताओं द्वारा दर्शाई जाती है:

- अपने जीवनचक्र के पहले नौ सालों में रैपिड एमिशन, जिसके दौरान **20,343,750 Epic** (कुल सप्लाई का **96.875%**) माइन होते हैं। इस दस्तावेज़ के एमिशन शेड्यूल भाग में बराबर एमिशन दरों को बताया गया है;
- **Epic** की चल सप्लाई और एमिशन दर **Epic** सिंगुलैरिटी पर बिटकॉइन के साथ सिंक हो जाती है लगभग **24** मई, **2028** तारीख के आसपास। सिंगुलैरिटी के बाद, एमिशन दर बढ़ती दर के हिसाब से घट जाती है, जबकि चल सप्लाई घटती दर पर बढ़ जाती है;
- साल **2140** तक **21** मिलियन **Epic** की अधिकतम सप्लाई लगभग उसी वक्त तक प्राप्त हो जाएगी, जब बिटकॉइन **21** मिलियन यूनिट की अधिकतम सप्लाई तक पहुंच जाएगा;
- **Epic** के पास **8** दशमलव की विभाजन संरचना है कि: **1 Epic 100,000,000 freeman** के बराबर है (वैसे ही जैसे **1** बिटकॉइन **100,000,000 satoshi** के बराबर है)।

इन कारणों से Epic Cash की मोनेटरी नीति बिटकॉइन की निति के बाद बनाई गई थी:

- बिटकॉइन के आर्थिक फंडामेंटलों के साथ मंजूरी, कि चल सप्लाई की कमी और पूर्वानुमान उसकी मजबूत मूल्य संचय गुणों के तहत हैं;
- पिछले दस सालों के दौरान जनता पहले से ही बिटकॉइन के तरीके और इसके सिद्ध ट्रैक रिकॉर्ड से परिचित है। लगभग बिटकॉइन की चल सप्लाई के साथ सिंक करके, और बिटकॉइन की अधिकतम सप्लाई और विभाजन संरचना का इस्तेमाल करके, **Epic** सबसे कम विरोध के साथ जन-समर्थन प्राप्त करना चाहता है।

VI. एमिशन शेड्यूल

Epic Cash के पास कुल में 33 माइनिंग युग हैं, और हर युग में ब्लॉक रिवॉर्ड कर्म हो जाता है, जो उनसे पहले से युग के संबंधित है। Epic जेनेसिस अगसत 2019 को होता है, जिस तार ख पर Epic ब्लॉक #1 का माइनिंग किया गया है। ब्लॉक हर मिनट माइन किए जाते हैं। पहले पाँच युगों में Epic की अधिकतम सप्लाई का लगभग 97% हिस्सा उत्पन्न होता है जो लगभग नौ वर्षों में बिटकॉइन एमिशन के 20 सालों की सप्लाई के समान है। यह उन लोगों के लिए 'इतिहास दोहराएगी' जिन्होंने बिटकॉइन की भव्य तरक्की को मिस कर दिया था।

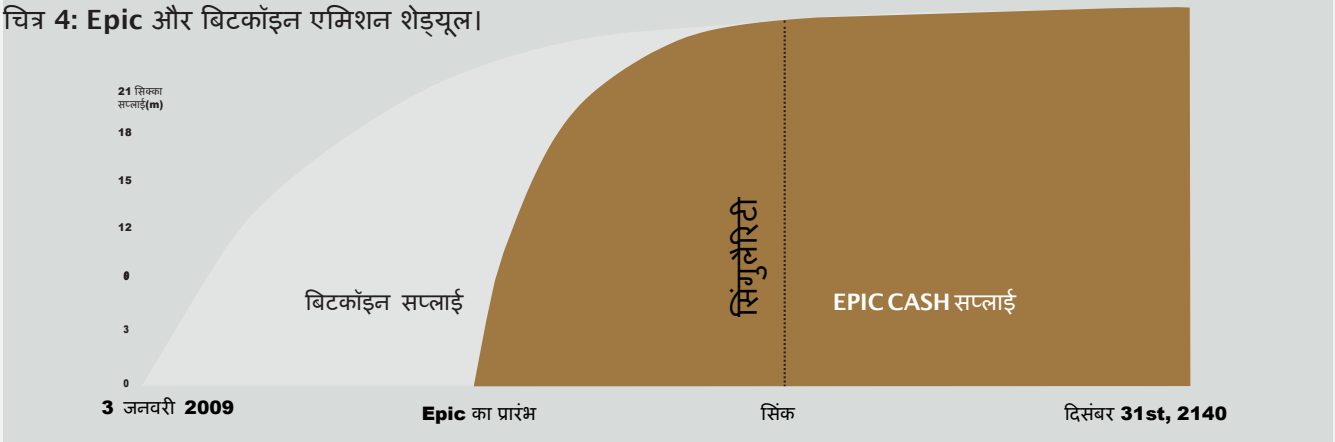
टेबल 1 एमिशन शेड्यूल सर्वप्रथम सात माइनिंग युगों की शुरुआत और अंतिम तारीखों, उनके संबंधित ब्लॉक रिवॉर्ड और हर युग के लिए आने वाली चल सप्लाई दर्शाती है। इस टेबल को छोटा रखने के लिए 8 से लेकर 33 युगों को टेबल में शामिल नहीं किया गया है। उन युगों के लिए, समझना आसान होना चाहिए कि ब्लॉक रिवॉर्ड उसके पहले के युग का आधा होगा, बिटकॉइन की तरह ही। इन हर युगों के दौरान, एमिट की गई Epic की संख्या ४-सालों (लगभग 1460 दिन) वाले युग के भीतर के ब्लॉक रिवॉर्ड का जोड़ होगा।

(2028) Epic सिंगुलैरिटी तक, Epic चल सप्लाई और बिटकॉइन की चल सप्लाई बराबर हो जाती है, जिस वक्त तक Epic Cash बिटकॉइन के ब्लॉक रिवॉर्ड और आधा होने के तरीके को अपनाता है, जो यह सुनिश्चित करता है कि हर चार साल में ब्लॉक रिवार्ड आधा हो जाता है। सिर्फ एक बात अलग है कि हर एक मिनट की दर पर Epic ब्लॉकों की माइनिंग प्रक्रिया जारी रहेगी, और बिटकॉइन का दर होगा हर दस मिनट में एक ब्लॉक। ऐसा करके, Epic चल सप्लाई बिटकॉइन की चल सप्लाई के साथ अपने बाकी के जीवनचक्र के लिए समानता बनाए रखती है।

टेबल 1: पहले सात माइनिंग युगों के लिए एमिशन शेड्यूल। तारीखें अनुमानित हैं।

युग	1	2	3	4	5	सिंगुलैरिटी	6	7
ब्लॉक रिवॉर्ड	16	8	4	2	1		0.15625	0.078125
शुरुआती तिथि	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
अंतिम तिथि	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
अवधि (दिनों में)	334	470	601	800	1019		1460	1460
शुरुआती सप्लाई	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
अंतिम सप्लाई	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
अधिकतम सप्लाई का %	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

चित्र 4: Epic और बिटकॉइन एमिशन शेड्यूल।



VII. माइनिंग

विभिन्न प्रकार के कंप्यूटर हार्डवेयर का इस्तेमाल करके **Epic Cash** ब्लॉकचेन डीसेंट्रलिज़ेशन की ओर बढ़ रहा है। तीन हैशिंग एल्गोरिदम का इस्तेमाल करके **Epic** माइनिंग शुरू-शुरू में **CPU**, **GPU** और **ASIC** के लिए उपलब्ध है**: RandomX, ProgPow,** और **CuckAToo31+**। एल्गोरिदम अपने आप स्वैप किए जा सकते हैं बिना चेन की अखंडता के साथ समझौता किए।

1 RandomX और CPUs

RandomX एक प्रूफ-ऑफ-वर्क **(PoW)** एल्गोरिथ्म है जो एक जनरल पर्पस **CPU** के लिए बना है। यह इन लक्ष्यों को हासिल करने के लिए कई मेमोरी-हार्ड तकनीकों के साथ-साथ रैंडमाईजड प्रोग्राम एक्सीक्यूश तरीके का इस्तेमाल करता है**:**

- एकल-चिप वाले **ASIC** के विकास पर रोक**;**
- जनरल पर्पस **CPU** पर विशिष्ट हार्डवेयर की दक्षता सुविधा को कम करना।

CPU के साथ **Epic** माइन करने के लिए हर माइनिंग थ्रेड के लिए **2 GB** फिजिकल **RAM**, **L1 cache** के **16 KB, L2 cache** के **256 KB** और **L3 cache** के **2 MB** के लगातार आवंटन की जरूरत पड़ती है[13]। विंडोज **10** के उपकरणों को **8 GB** या अधिक **RAM** की जरूरत है। वह दिन अभी दूर नहीं है कि मोबाइल फोन भी माइनिंग नोड बनेंगे। **Epic Cash** माइनिंग नेटवर्क में **CPU** को शुरुआत से ही एकीकृत करना एक बढ़िया तरीका है जिसमें सस्ते कंप्यूटिंग साधनों के साथ ब्लॉक रिवार्ड कमाया जा सकता है जिससे **Epic Cash** नेटवर्क को सुरक्षित किया जा सकता है।

2 ProgPow और GPUs

प्रोग्रामेटिक प्रूफ-ऑफ-वर्क (**ProgPow**) एक ऐसा एल्गोरिथ्म है जो मेमोरी बैंडविड्थ और रैंडम मैथ सीक्वेंस की गणना पर निर्भर करता है**,** जो **GPU** की कई कंप्यूटिंग सुविधाओं का इस्तेमाल करते हैं और इस तरह हार्डवेयर की कुल एनर्जी लागत कम होती है। क्योंकि **ProgPow** विशेष रूप से कमोडिटी **GPU** का पूरा इस्तेमाल करने के लिए बनाया गया है**,** खास तौर से बनाए गए हार्डवेयर की मदद से उच्च क्षमता प्राप्त करना मुश्किल और महंगे दोनों हैं। फिलहाल**, ProgPow** एल्गोरिथ्म बड़े **ASIC** पूल के लिए प्रोत्साहन राशियों को कम करता है ताकि वह **GPUs** से बेहतर बन सके**,** जैसे कि कई अन्य **PoW** एल्गोरिदम**,** जैसे **Bitcoin** के **SHA-256** के मामले में देखा गया है। **GPU,** हालांकि **CPU** की तरह लोकप्रिय नहीं हैं**,** फिर भी आमतौर से उपलब्ध हैं। पावरहाउस जैसे **Nvidia** और **AMD** द्वारा प्रेरित तकनीकी विकास के साथ**, GPU** प्रति यूनिट के आधार पर **CPU** से अधिक अनेक माइनिंग तरीकों को साथ में प्रोसेस करने की क्षमता रखते हैं। **GPU** के इस यूबिक्विटी और उच्च प्रोसेसिंग क्षमता के जोड़ के कारण वह टेबल 2 में दर्शाए गए शुरुआती युगों के दौरान की गई माइनिंग गतिविधि का आधार बनेगा।

3 CuckAToo+31 और ASICs

इच कंप्यूटर वैज्ञानिक**, John Tromp,** ने **Cuckoo Cycle** एल्गोरिथ्म **CuckAToo31 +** नामक एक **ASIC** अनुकूल एल्गोरिथ्म को तैयार किया। **ASIC** रेसिस्टेंट **CuckARoo29** से संबंधित**, CuckAToo31 +** रैंडम द्वो भागों वाले ग्राफ को उत्पन्न करता है और माइनरों को दी गई लम्बाई "**N**" के लूप को ढूंढने के काम में लगा देता है जो उस ग्राफ के सिरे से होकर गुज़रता है।

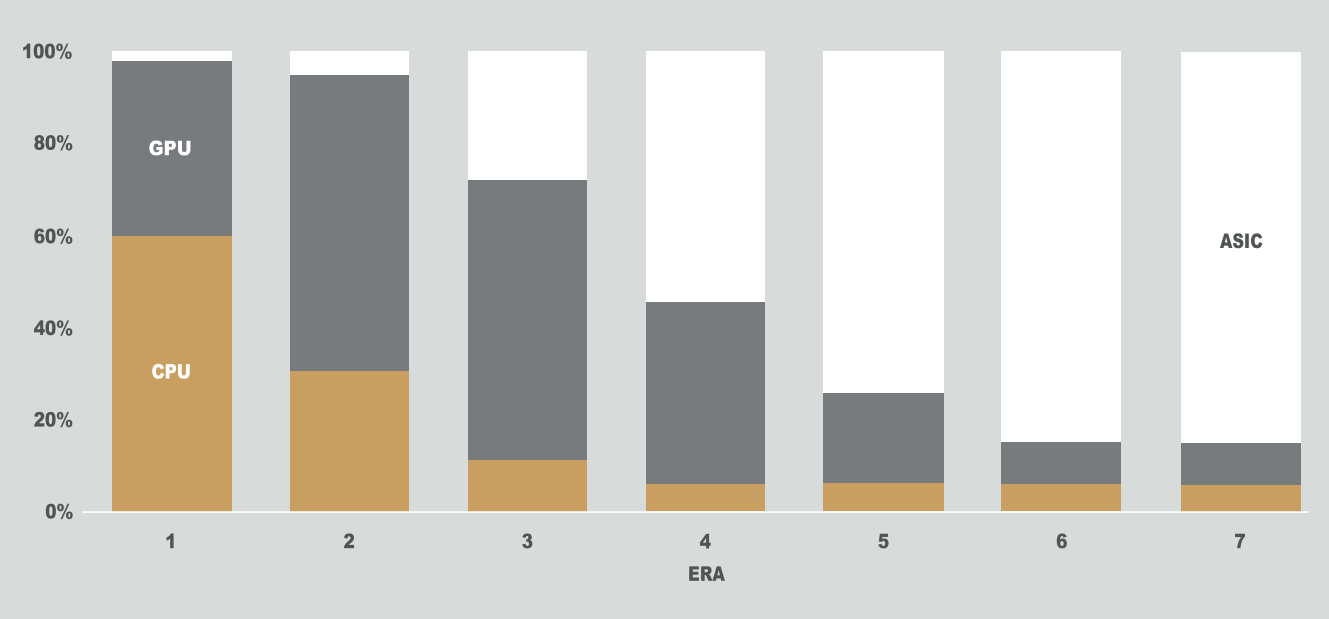
[13] **Tevador,** *RandomX*, **28 March, 2019,** https://github.com/tevador/RandomX

यह एक मेमोरी से बंधा कार्य है, यानी कि समाधान का समय मेमोरी बैंडविड्थ से बंधा है न कि रॉ प्रोसेसर या **GPU** स्पीड से। नतीजतन, **Cuckoo Cycle** एल्गोरिदम कम गर्मी पैदा करते हैं और पारंपरिक **PoW** एल्गोरिदम की तुलना में काफी कम एनर्जी का इस्तेमाल करते हैं। **ASIC-**अनुकूल **CuckATOO31+ GPU** पर बेहतर दक्षता प्रदान करते हैं जिसके लिए वे **SRAM** के सैकड़ों **MB** का इस्तेमाल करते हैं और इस दौरान वे मेमोरी **I/O** की बाधाओं से झुंझते हैं [14]। अंत में, **ASIC** तीनों माइनिंग विकल्पों के पैमाने की सबसे बेहतर आर्थिक क्षमता पेश करते हैं। भाग लेने के इरादे से, उन्हें शुरुआत में **CPU** और **GPU** के मुकाबले माइनिंग पुरस्कारों का एक छोटा हिस्सा दिया जाता है, लेकिन अंत में **ASIC** माइन किए गए ब्लॉक रिवॉर्ड के एक बड़े हिस्से को प्राप्त करते हैं, इस मान्यता पर कि **CuckATOO31+** कई डिवाइस निर्माताओं द्वारा समर्थित होगी।

टेबल 2: माइनिंग पुरस्कार के आवंटन। बदलाव के अधीन। अधिकतम डीसेंट्रलिज़ेशन और नेटवर्क के आगे के हितों को ध्यान में रखते हुए आवंटन को निर्धारित किया जाएगा।

युग	1	2	3	4	5	6	7
Days	**334**	**470**	**601**	**800**	**1019**	**1460**	**1460**
CPUs	**60%**	**30%**	**10%**	**5%**	**5%**	**5%**	**5%**
GPUs	**38%**	**65%**	**62%**	**40%**	**20%**	**10%**	**10%**
ASICs	**2%**	**5%**	**28%**	**55%**	**75%**	**85%**	**85%**

चित्र 5: टेबल 2 के अनुसार हर युग के लिए माइनिंग इनामों का आवंटन। बदलाव के अधीन।



[14] **Le Sceller, Quentin,** *An Introduction to Grin Proof-of-Work,* **16 November, 2018,** https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 माइनिंग के योगदान

Epic जेनेसिस **(2019)** से शुरुआत करके और **Epic** सिंगुलैरिटी **(2028)** तक समाप्त होकर**,** माइनिंग प्रक्रिया के दौरान**, Epic** का एक हिस्सा **EPIC** ब्लॉकचेन संस्था के लिए माइनिंग योगदानों के रूप में आवंटित किया जाएगा।
EPIC ब्लॉकचेन संस्था तकनीकी विकास का काम करती है और फाइनेंसियल तकनीकी उद्योग में मार्केटिंग गतिविधियों और साझेदारियों की मदद से **Epic Cash** प्रोजेक्ट की उपयोगिता के लिए उसके शुरुआती सालों से ही जागरूकता बढ़ाने का काम करती है।
सिंगुलैरिटी के बाद**, EPIC** संस्था का कार्य अब **EPIC** डिस्ट्रीब्यूटेड ऑटोनोमस कॉर्पोरेशन (**EDAC)** की जिम्मेदारी होगी**,** जो सौंपने से पहले संस्था द्वारा विकसित होगी।
EPIC ब्लॉकचेन संस्था को इन सालाना दरों के अनुसार माइनिंग रिवॉर्ड का प्रतिशत दिया जाता है**,** जो ब्लॉक रिवॉर्ड से घटाया जाता है**:**

टेबल 3: माइनिंग रिवॉर्ड के प्रतिशत के रूप में संस्था के माइनिंग योगदानों के वार्षिक दर।

साल	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
माइनिंग पुरस्कारों का%	**8.88 %**	**7.77 %**	**6.66 %**	**5.55 %**	**4.44 %**	**3.33 %**	**2.22 %**	**1.11 %**	**1.11 %**	**0 %**

VIII. निष्कर्ष

Epic, एक्सचेंज के साधन के रूप में, 'डीसेंट्रलाइज्ड डिजिटल का चांदी' बनना चाहता है**,** जैसे कि बिटकॉइन को डीसेंट्रलाइज्ड डिजिटल सोने के रूप में पहचान दी गई है। अनुपलब्ध फंगिबिलिटी को और अधिक एनर्जी इफिशियंट और एको-फ्रेंडली हार्डवेयर के साथ फिर से लाकर**, Epic Cash** फिर से उपयोगकर्ताओं को इसपर नियंत्रण देता है जो आज के सेंट्रलाइज्ड नेटवर्क से बिलकुल अलग है। बिटकॉइन की आर्थिक स्थिति**,** खेल सिद्धांत**,** और सिद्ध प्रूफ-ऑफ़-वर्क फार्मूला को सबसे बेहतर ब्लॉकचेन तकनीक के साथ जोड़कर**,** एक भरोसेमंद**,** अपरिवर्तनीय और डीसेंट्रलाइज्ड मुद्रा **(Epic)** उत्पन्न होता है जो स्केलेबल**,** फंगिबिल है**,** और जो अपने उपयोगकर्ताओं की प्राइवेसी की रक्षा करता है। **Epic Cash** ब्लॉकचेन खुला**,** सार्वजनिक**,** सीमा-रहित और सेंसरशिप-प्रतिरोधी है। यह अपने उपयोगकर्ताओं की प्राइवेसी और धन की रक्षा करता है और यह माइनिंग के जरिये अपने हार्डवेयर को नेटवर्क के लिए इस्तेमाल करने वाले लोगों को पुरस्कार देता है। हर **Epic** को प्रूफ-ऑफ़-वर्क के जरिए बनाया जाता है। शून्य से सप्लाई की शुरुआत होती है और नेटवर्क के लांच को उचित माना जाता है**,** जिसमें एक काम करने वाला टेस्टनेट फिलहाल चल रहा है।

Epic Cash के मुख्य तथ्य:

- अगसत**, 2019** से र्माइनिंग शुरू होता है।
- **MimbleWimble** पर **Epic Cash** ब्लॉकचेन आधारित है।

  प्रोटोकॉल की विशेषताएं इस प्रकार हैं:

  1. ***कट-थ्रू*** – जगह बचत को बढ़ावा देने के लिए ब्लॉकचेन से अनावश्यक जानकारी को हटाना, नेटवर्क वेलिडेशन में बड़े पैमाने पर भागीदारी को बढ़ावा देना और डीसेंट्रलिज़ेशन का प्रबंधन करना;
  2. ***CoinJoin*** - Epic क्रिप्टोमुद्रा की फंजिबिलिटी सुनिश्चित करने के लिए एक ब्लॉक में सौदों को इकठ्ठा करना;
  3. ***Dandelion++*** प्रोटोकॉल – एक साथ जुड़े चैनलों के पार संचार करके, और नोडों के एक बड़े नेटवर्क में फैलाकर, सौदों और उनके ओरिजिन के बीच कनेक्शन को अलग करके सौदों का प्रसार करना;
  4. **कोई वॉलेट पते नहीं** – सौदा करने वाले दलों के लिए एकल-प्रयोग वाली प्राइवेट चाबियों को उत्पन्न करने के लिए बड़े बहु-हस्ताक्षर का इस्तेमाल करना, जिससे वॉलेट के पतों की आवश्यकता कम हो जाती है।

- लगभग नौ सालों में **Epic** और बिटकॉइन के चल सप्लाई को सिंक करने के लिए और साल **2140** में बिटकॉइन की तरह **21** मिलियन यूनिट की अधिकतम सप्लाई प्राप्त करने के लिए, **Epic Cash** की मोनेटरी नीति को तैयार किया गया है। यह घटती इन्फ्लेशनरी निति ट्रांसपेरेंसी**,** सप्लाई का अनुमान लगाने की योग्यता**,** और अभाव का आश्वासन देती है**,** जिससे आगे चलकर मूल्य संचय की सुरक्षा को बढ़ावा मिलता है।

- माइनिंग जो **RandomX, ProgPow,** और **CuckATOO31+** एल्गोरिदम के जरिये **CPU, GPU** और **ASIC** को शामिल करता है**,** ताकि जन-समर्थन और नेटवर्क दक्षता को सुविधाजनक बनाया जा सके।

IX. तकनीकी निर्देश

प्रोजेक्ट का नाम: **Epic Cash**

मुद्रा का नाम: **Epic**

ब्लॉक समय: **60** सेकंड

ब्लॉक साइज़: **1 MB**

शुरुआती सप्लाई: **0**

अंतिर्म सपलाई: **21,000,000**

जेनेसिस ब्लॉक: अगसत, **2019**

कन्सेंसस: **RandomX (CPUs), ProgPow (GPUs)** और **CuckAToo31+ (ASICs)**

लिंक:

www.epic.tech

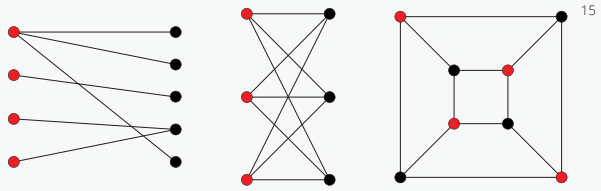
t.me/EpicCash - **टेलीग्रार्म**

t.me/EpicCashHindi

X. शब्दकोष

ASIC एप्लीकेशन स्पेसिफिक इन्टग्रेटिड सर्किट; चिप्स जिन्हें एक एकल उद्देश्य के लिए तैयार किया गया है।

दो भागों वाला ग्राफ ग्राफ सिरों का एक सेट जिन्हें दो अलग-अलग सेट में अलग किया जाता है, इस प्रकार कि कोई भी दो ग्राफ सिरे एक ही सेट में एक-दूसरे के बगल में न हो।



ब्लाइंडिंग कारक एन्क्रिप्शन की सुविधा देने के लिए एक डिजिटल संदेश में एक रैंडम तत्व शामिल किया जाता है; दो दलों के बीच एक शेयर्ड सीक्रेट जो एक खास सौदे में इनपुट और आउटपुट को और साथ ही सौदा करने वाले दलों के प्राइवेट और पब्लिक चाबियों को एन्क्रिप्ट करता है।[16]

ब्लॉक रिवॉर्ड एक नए ब्लॉक में सौदे को वेरीफाई करने के लिए की गई गणनाओं के लिए पुरस्कार के रूप में नेटवर्क द्वारा बांटे नए **Epic**।

Cache एक हार्डवेयर या सॉफ्टवेयर तत्व जो डेटा को स्टोर करता है ताकि उस डेटा के लिए भावी अनुरोध तेजी से किए जा सके।

चल सपलाई एक निश्चित समय पर **Epic** की वास्विक मात्रा।

CPU सेंट्रल प्रोसेसिंग यूनिट: कंप्यूटर के अन्य हार्डवेयर और सॉफ्टवेयर से अधिकतर कमांड का मतलब समझाने और पूरा करने के लिए जिम्मेदार, कंप्यूटर का एक घटक।

कट-थरू एक **MimbleWimble** ब्लॉकचेन प्रक्रिया जिसमें इनपुट और मेल खाने वाले खर्च आउटपुट को ब्लॉक में जगह खाली करने के लिए हटा दिया जाता है, जिससे ब्लॉकचेन पर स्टोर करने के लिए जरूरी डेटा की संख्या को कम किया जाता है।

ड सेंट्रलिज़ेनश किसी नेटवर्क के संचालन और नियंत्रण के फैलाव की स्थिति।

एर्मिनश ब्लॉक रिवॉर्ड में माइनरों द्वारा कमाए नए **Epic** का निर्माण। ब्लॉकचेन में जैसे-जैसे सौदे पुष्ट होते हैं वैसे ही **Epic** हर **60** सेकंड उत्पन्न होते हैं।

Epic सिंगुलैरिट वह समय जब **Epic** की चल सप्लाई बिटकॉइन की चल सप्लाई (मई **2028)** के साथ सिंक होती है।

अतिरिक्त (**MimbleWimble)** आउटपुट और इनपुट के बीच का अंतर और साथ ही हस्ताक्षर (ऑथेंटिकेशन के लिए और गैर-इन्फ्लेशन साबित करने के लिए)।

फंगिबिलिट किसी वस्तु का एक ऐसा गुण जिसके तहत व्यक्तिगत इकाइयां अनिवार्य रूप से बदलने योग्य हैं, और इसका हर एक भाग दूसरे भाग से अलग दिखाई नहीं देता है।

जेनेसिस (घनटा) पहले **Epic** ब्लॉक का माइनिंग और ब्लॉकचेन की आधिकारिक स्थापना।

GPU ग्राफिक्स प्रोसेसिंग यूनिट: एक यूनिट जिसमें डिस्प्ले कार्यों के लिए खास तौर से बनाया गया प्रोग्रामेबल चिप (प्रोसेसर) शामिल है। क्रिप्टोमुद्रा माइनिंग के लिए उपभोक्ता **GPU** सबसे उपयुक्त हैं।

अर्धिकरण (बिटकॉइन के लिए) हर **4** साल में होता है। हर एक अर्धिकरण कार्यक्रम के बाद सप्लाई की दर **50%** से घट जाती है।

हैश हैशिंग फ़ंक्शन का इस्तेमाल कर एक बेस इनपुट अंक से गणना किया गया मूल्य।

हाशिंग एलगोरिथर्म (फ़ंक्ट्नश) मैथमेटिकल एल्गोरिदम जो आर्बिट्रेरी साइज़ के डेटा को एक फिक्स्ड साइज़ के हैश से जोड़ता है

होर्मोर्मोर्फिक एर्क्रिपनश जिसका इस्तेमाल डिजिटल हस्ताक्षरों, मेसेज ऑथेंटिकेशन कोड (**MAC**), और ऑथेंटिकेशन के अन्य रूपों को उत्पन्न करने और वेरीफाई करने के लिए होता है।

प्राइवेसी संरक्षित करने के लिए एन्क्रिप्टेड जानकारी पर, उसे डिक्रिप्ट किए बिना, गणना करने का एक तरीका।

अपरिवर्तनीय (प्रोग्रामिंग में) वह स्थिति जिसमें किसी वस्तु को उसके निर्माण के बाद बदला नहीं जा सकता।

इनपुट (**MimbleWimble)** **MimbleWimble** सौदे का घटक जो सौदा भेजने वाले दल को रिप्रेजेंट करता है; पिछले सौदों के आउटपुट से बनाया गया।

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] **Macdonald, Andrew,** *Grin Coin and MimbleWimble: An Introductory Guide*, **18 October, 2018,** https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

I/O इनपुट/आउटपुट**;** एक सूचना प्रोसेसिंग व्यवस्था के बीच का संचार**,** जैसे कि एक कंप्यूटर और बाहरी दुनिया**,** जैसे मानलो एक मानव या अन्य सूचना प्रोसेसिंग व्यवस्था।

अधिकतम सप्लाई **Epic** की संख्या जिसे प्राप्त करना है**,** और उस वक्त के बाद चल सप्लाई नहीं बढ़ेगी **(21,000,000 Epic)**।

मेमोरी-हार्ड बहुत सारे **RAM** का इस्तेमाल**,** ताकि समकालिक (साइमल्टेनीअस) कनेक्शन को रोका जाए कि वे एक साथ प्रयासों को न चलाए। मेमोरी-हार्ड फ़ंक्शंस ऐसे एल्गोरिदम हैं जिनकी गणना का समय मुख्य रूप से उपलब्ध मेमोरी द्वारा निर्धारित होता है जिसके लिए डेटा रखा जाता है। मेमोरी-बंधे फ़ंक्शन के नाम से भी जाने जाते हैं।

मर्कल ट्री कंप्यूटर विज्ञान एप्लीकेशनों में प्रयुक्त एक डेटा संरचना। ब्लॉकचेन में**,** मर्कले ट्री बड़ी डेटा संरचनाओं में कंटेंट की निपुण और सुरक्षित वेरिफिकेशन में मदद करते हैं।

MimbleWimble एक बिटकॉइन डेवलपरों के चैटरूम में **Tom Elvis Jedusor** के नाम से पहचाने जाने वाला एक अज्ञात योगदानकर्ता द्वारा पेश किया गया एक [प्रोटोकॉल](#)।

बहु-हस्ताक्षर एक डिजिटल हस्ताक्षर योजना जो कई उपयोगकर्ताओं को एक ही दस्तावेज़ पर हस्ताक्षर करने में मदद करता है। आमतौर पर**,** एक बहु-हस्ताक्षर एल्गोरिथ्म एक जॉइंट हस्ताक्षर बनाता है जो सभी उपयोगकर्ताओं के अलग-अलग हस्ताक्षर के कलेक्शन से अधिक ठोस होता है।

नोड एक कंप्यूटर जो एक ब्लॉकचेन नेटवर्क से जुडता है और एक पीयर-से-पीयर तरीके में सौदों और ब्लॉकों के बारे में जानकारी बांटने के लिए नेटवर्क के अंदर दूसरे नोडों तक पहुँचता है।

वन-वे एगरीगेट सिगनेचर **(OWAS)** कई हस्ताक्षरों से बना एक लेनदेन हस्ताक्षर**,** जो इस तरह एन्क्रिप्ट किया जाता है**,** ताकि समूह के एक हिस्सा में शामिल व्यक्तिगत हस्ताक्षरों की गणना करना मुश्किल हो जाए।

आउटपुट **(MimbleWimble)** पेडर्सन **MimbleWimble** सौदे का हिस्सा जो सौदे की प्राप्ति को दर्शाता है**;** जिसे आने वाले सौदों के लिए इनपुट की तरह इस्तेमाल किया जाता है।

कर्मिटमैंट सकीर्म एक क्रिप्टोग्राफ़िक प्रिमिटिव जो एक प्रूवर को एक चयनित मूल्य को निर्धारित करने में मदद करता है बिना किसी जानकारी का खुलासा करे**,** और बिना प्रूवर को उस मूल्य को निर्धारित करने के कार्य को नकारने का मौका दिए।

पराइवेट की एक प्राइवेट चाबी (की) कोड का एक छोटा सा भाग है जिसे पब्लिक की के साथ जोड़ा जाता है ताकि टेक्स्ट के एन्क्रिप्शन और डीक्रीपशन के लिए अल्गोरिथम नियुक्त किए जा सके। इसे एसिमेट्रिक चाबी के एन्क्रिप्शन के दौरान पब्लिक चाबी क्रिप्टोग्राफी के हिस्से के रूप में बनाया गया है और एक पढने योग्य फॉर्मेट में सन्देश को डिक्रिप्ट और बदलने के लिए इस्तेमाल किया गया है।

परूफ-ऑफ़-वर्क **(PoW)** डेटा का एक हिस्सा जिसे पैदा करना मुश्किल है (महंगा और समय लेने वाला कार्य)**,** लेकिन दूसरों के लिए वेरीफाई करना आसान है**,** और जो कुछ जरूरतों को पूरा करता है। प्रूफ-ऑफ़-वर्क अक्सर क्रिप्टोमुद्रा ब्लॉक को पैदा करने में इस्तेमाल किए जाते हैं।

पब्लिक चाबी एक पब्लिक चाबी एन्क्रिप्शन क्रिप्टोग्राफ़ी में पब्लिक चाबी बनाई जाती है जिसके लिए एसिमेट्रिक चाबी के एन्क्रिप्शन की प्रक्रिया की जाती है। पब्लिक चाबियों का उपयोग किसी संदेश को अस्पष्ट फॉर्मेट में बदलने के लिए किया जाता है।

रेंजपरूफ एक कमिटमेंट वेलिडेशन**,** जो पुष्टि करता है कि सौदे के इनपुट का जोड़ सौदे के आउटपुट के जोड़ से ज्यादा है और कि लेनदेन के सभी अमाउंट पॉजिटिव हैं। रेंजप्रूफ यह सुनिश्चित करते हैं कि मोनेटरी सप्लाई के साथ कोई छेड़छाड़ नहीं की गई है।

RAM (रैंडर्म एक्ट्सेस मैर्मोर **)** एक कंप्यूटिंग डिवाइस में फास्ट-एक्सेस डेटा स्टोरेज के चिप जहां ऑपरेटिंग सिस्टम **(OS),** एप्लिकेशन प्रोग्राम और वर्तमान में इस्तेमाल किया जाने वाला डेटा रखा जाता है ताकि डिवाइस के प्रोसेसर उनतक जल्दी से पहुंच सकें।

(डिजिटल) हसताक्षर ब्लॉकचेन प्रोटोकॉल का एक आम हिस्सा जिसे मुख्य रूप से सौदों और सौदे के ब्लॉकों**,** जानकारी के ट्रांसफर**,** कॉन्ट्रैक्ट प्रबंधन को सुरक्षित रखने और किसी भी अन्य मामलों को सुरक्षित रखने के लिए इस्तेमाल किया जाता है जहां किसी भी बाहरी छेड़छाड़ के बारे में जानना और रोकना जरूरी है। ब्लॉकचेन पर जानकारी को स्टोर करने और ट्रांसफर करने के तीन फायदे वे पेश करते हैं:

- वे बताते हैं कि क्या भेजे जा रहे डेटा के साथ कोई छेड़छाड़ की गई है**;**
- वे सौदे में किसी खास दल की भागीदारी को वेरीफाई करते हैं**;**
- कानूनी रूप से बाध्यकारी हो सकते हैं।

SRAM (सटेटिक रैंडर्म एक्ट्सेस मैर्मोर) थरूपुट रैंडम एक्सेस मेमोरी **(RAM)** जो अपने मेमोरी में डेटा बिट रखता है सिर्फ तब तक जब तक कि बिजली प्रदान की जा रही है।

हर सेकंड लेनदेन का माप जो कोई भी क्रिप्टोमुद्रा प्रोटोकॉल कर सकता है।

ट्रसटलिसनिस किसी केंद्रीय दल के दबाव के बिना किसी प्रोटोकॉल के नियमों का पालन करने की एक क्रिप्टोमुद्रा नेटवर्क की खासियत।

[17] **Bellare, Mihir, Neven, Gregory, 2007,** *Identity-based Multi-signatures from RSA*, **Lecture Notes in Computer Science vol. 4377,** https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH