Pamilya ni Freeman

July 4, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Isang Peer-to-Peer Electronic Cash na System

PAGIIMBAK NG HALAGA + KAGAMITAN SA PAGPAPALITAN + BATAYAN NG BILANG

1.7 na bilyong katao ang hindi na kakagamit ng pandaigdigang pampinansyal na sistema, habang ang ibang 1.3 na bilyon ay hindi naseserbisyohan. Ang potensyal ng tao dito ay binuksan ng Epic Cash sa pamamagitan ng pagkonekta ng mga indibiwal sa pandaigdigang merkado. Mabilis, libreng magagamit, at bukas para sa lahat.

Version 7.1b

II. Pagkapribado

Ang mordernong paggamit ng pananalapi ay mauunawaan tulad ng kolektibong pagsasalin ng mga bilang ng account sa pagitan ng mga tao at mga institusyon. Ang lugar ng pananalapi sa anumang naibigay na oras ay maaaring mai-map sa pamamagitan ng pagsagot sa mga sumusunod na katanungan:

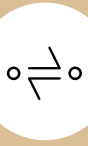
1. *Sino ang may hawak nito, at ilang ang hawak nila?*
2. *Kanino siya nakikipagtransaksyon, at magkano ito?*

Para sa mga tradisyunal na pananalapi, at sa katotohanan din ng Bitcoin, masasagot natin ang mga katanungang iyon. Sa paggawa nito, marami ang mabubunyag tungkol sa pamumuhay ng mga tao, tulad ng mga pagkonsumo, pagmamay-ari, at mga transakyon ng katapat. Ang makatarungang na mga konklusyon ay maaaring makuha tungkol sa mga interes at hangarin ng isang indibidwal sa pamamagitan ng pagsubaybay sa mga halaga na inililipat. Kung walang pagkapribado, ang datos ng transaksyon ay maaaring mapanganib na impormasyon sa mga kamay ng mga mapanganib na third parties.

Ang nakaraang dekada ng paggamit ng cryptocurrency ay nagpapakita ng pagpapatuloy ng "pagkapribado" sa iba't ibang mga pagpapatupad ng blockchain. Ang sukat ng pagkapribado, dapat isaalang-alang, nasasaklaw mula sa bukas at kilala tungo sa isang dulo hanggang sa hindi ito nakikilala. Habang tumatagal ang pagkapribado, isang mahalagang pundasyon ng cryptocurrency, walang mapagkatiwalaan, pinanghihinalaan. Tulad ng napatunayan ng tagumpay ng mga serbisyo ng pagsusuri sa blockchain ng Bitcoin, Ang Bitcoin ay matatag ang pagkakakilanlan sa pagtatapos ng spectrum ng pagkapribado. Ang mga gumagamit ay dapat na patuloy na gumawa ng mga hakbang upang matiyak na hindi nila sinasadyang gumagawa ng transakyon sa masungit na halaga ng Bitcoin. Ang solusyon ng Epic Cash ay natauon patungo sa pagka-anonimo at ibalik ang mahahalagang ari-arian sa pamamagitan ng pagtiyak ng pagkapribado ng indibidwal at pagkapribado ng mga transaksyon ay isinasaayos sa system sa napakahalagang antas.

Pagkapribado ng Pagkakakilanlan

Pagkapribado ng Transaksyon



Pagkapribado ng Pagkakakilanlan

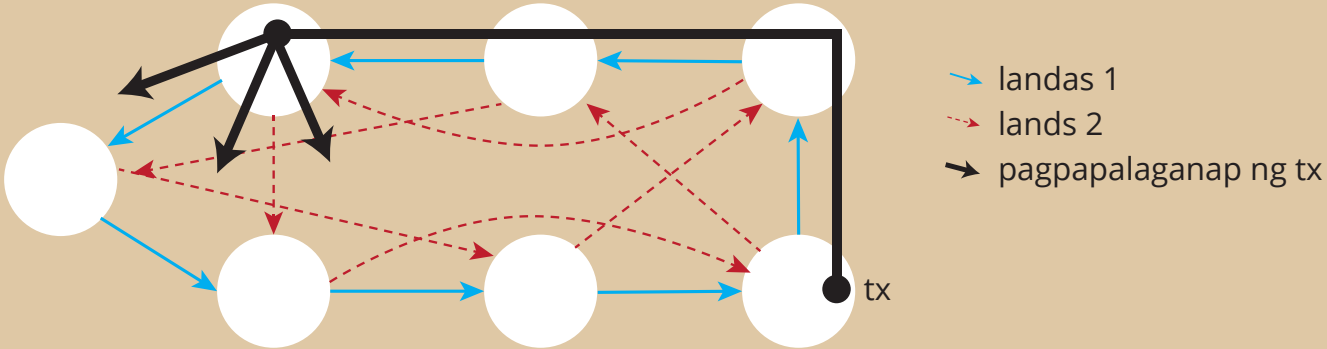
Karamihan sa mga cryptocurrencies tulad ng Bitcoin ay naka-imbak sa mga pitaka na ang mga address ay tumutukoy sa mga public key na nagmula sa mga private key ng isang pitaka. Ang mga address na ito ay maaaring isipin bilang mga tagahanap ng private vault ng digital na mundo. Ang blockchain ng Epic Cash ay tinatanggal ang mga address nang lubusan at sa halip ay inilalapat ang isang grand multi-signature na kung saan ang lahat ng public at private key ay nabuo sa isahangpaggamit.

Dahil ang mga address ng Bitcoin wallet ay tagahanap ng isang vault sa digital na mundo, ang pitaka na iyon ay maaaring masubaybayan sa isang address ng Internet Protocol (IP) ng isang may-ari, na kung saan ang anchor ang may-ari sa isang computer sa isang natatanging lokasyon sa isang takdang oras. Ipinaliwanag lamang: kapag naganap ang isang transaksiyon sa Bitcoin, ang transaksyon ay naipahayag mula sa isang hub ng komunikasyon na tinatawag na isang 'node' at pagkatapos ay ipinapalaganap sa iba pang mga node na tinatawag na 'peers'. Mabilis na kumakalat ang impormasyong iyon sa bawat isa sa mga kapantay na mga node nang sunud-sunod sa buong network. Ang prosesong ito ay angkop na pinangalanang "Gossip Protocol". Sa madaming salita, ang bawat Bitcoin ay may nakikitang posisyon sa online at isang pisikal na lokasyon kung nasaan ito, o sa halip ang may-ari ng Bitcoin, ay matatagpuan. Tulad ng nabanggit ng mamamahayag na si Grace Caffyn, ang Bitcoin ay "walang lihim kaysa sa Google search mula sa isang koneksyon sa internet sa bahay."[2]

Bilang karagdagan sa pagtatanggal ng mga wallet address, ang blockchain ng Epic Cash ay tinitiyak na ang pagkapribado ng pagkakakilanlan sa pamamagitan ng pagtiyak ay hindi masusubaybayan sa pamamagitan ng IP address. Gagawin ito sa pamamagitan ng pagsasama ng **Dandelion ++ Protocol**. Ang pagpapabuti sa nauna rito, ang orihinal na **Dandelion Protocol**, ang **Dandelion ++ Protocol** ay resulta ng pitong patuloy na gawain ng mga mananaliksik upang labanan ang mga pag-atake ng deanonymization sa blockchain. Sa pamamagitan ng **Dandelion ++**, ang mga transaksyon ay ipinasa sa mga random na intertwined path, o 'cables', at pagkatapos ay biglang nagkalat sa isang malaking network ng node, tulad ng mga pods ng isang bulaklak ng Dandelion kapag pinutok mula sa kanilang tangkay (Larawan 1). Gagawin nitong halos imposible na masubaybayan ang mga transaksyon pabalik sa kanilang pinagmulan, at sa gayon din ang pinagmulan ng mga IP address.

Larawan 1: Pag-aanomino ng Transaksyon gamit ang *Dandelion++ Protocol.*

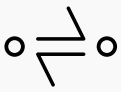
Ang Dandelion ++ ay naghahatid ng mga mensahe sa isa sa dalawang magkakaugnay na mga landas sa isang 4-regular na graph pagkatapos ay naipahayag ang gamit pagkalat. Sa larawan, ang transaksyon ay nagpapalaganap sa asul na solidong landas[3]. Napakahirap ng prosesong ito na masubaybayan ang mga transaksyon pabalik sa kanilang mapagkukunan, sa gayon pinapanatili ang pagkapribado.



[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

Pagkapribado ng Transaksyon



Ang blockchain ng Epic Cash ay tinitiyak na ang pagkapribado ng transaksyon sa pamamagitan ng pagkubli ng halaga at ang relasyon ng nagpadala-tatanggap ng isang transaksyon. Ito ay nakamit sa pamamagitan ng aplikasyon ng mga ideya na pamilyar mula sa Confidential Transaction[4] (CT) at CoinJoin[5], mga pamamaraan sa malaking bahagi na binuo ni Gregory Maxwell (developer ng Bitcoin Core, Co-Founder, at CTO ng Blockstream).

Ang CT, na orihinal na nilikha ni Adam Back at kalaunan ay pinino ng Maxwell, ay gumagana sa pamamagitan ng pagsira sa mga transaksyon sa mas maliit na bahagi sa pamamagitan ng homomorphic encryption, isang paraan ng pagsasagawa ng mga kalkulasyon sa naka-encrypt na impormasyon nang hindi nai-decrypt muna upang mapanatili ang pagkapribado. Kapag nahati ito, hindi nakikita ng mga tagamasid ang aktwal na halaga ng mga transaksyon dahil sa mga blinding factors, isang sistema na nagtatapon ng mga random na numero sa halo ng mga fragment ng transaksyon upang maitago ang mga halaga ng mga fragment. Sa huli, ang mga transacting party lamang ang nakakaalam ng halaga ng isang palitan, habang ang transaksyon ay naberipika ng network sa pamamagitan ng kumpirmasyon na ang kabuuan ng mga halaga ng output ay katumbas ng kabuuan ng mga halaga ng pag-input, at ang kabuuan ng mga output ng blinding factors ay katumbas ng kabuuan ng mga input ng blinding factors.

Upang maging higit pang kumplikado ang gawain ng mapagmasid na mata, ang lahat ng mga transaksyon sa Epic Cash ay tinatago sa CT at pagkatapos ay pinagsama-sama upang itago ang mga koneksyon sa pagitan ng mga magkatransaksyon partido. Ito ay gagawin sa pamamagitan ng pangalawang konsepto ni Maxwell, ***CoinJoin***.

Ang simpleng paglalarawan sa ***CoinJoin***, isipin na ang A, B, at C ay nagpapadala ng Epic sa X, Y, at Z, ayon sa pagkakabanggit. Ipinadala sa pamamagitan ng CoinJoin medium, ang lahat ng kilala ay ang A, B, at C ay nagpapadala at ang X, Y, at Z ay tumatanggap, habang ang mga halaga ng transaksyon ay mananatiling hindi nakikita. Ang sistema ng CoinJoin ay pangunahing sa Epic Cash sa pamamagitan ng One-Way Aggregate Signature (OWAS), na pinagsasama ang lahat ng mga transaksyon sa loob ng isang block sa pamamagitan ng isang transaksyon.

Pagkapribado: Buod

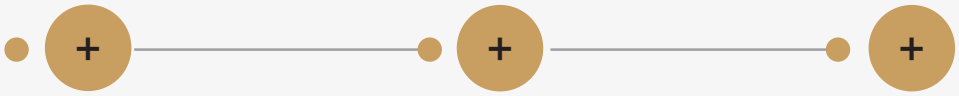
Ang blockchain ng Epic Cash ay pinoprotektahan ang pagkapribado ng mga indibidwal at ang kanilang mga transaksyon sa pamamagitan ng:

- **Pag-aalis ng mga wallet address** – Twalang lokasyon dito na malalaman sa digital vaults sa loob ng blockchain. Ang mga transaksyon ay ginawa direkta sa tao-sa-tao sa wallet-sa-wallet na batayan.
- ***Con idential Transactions*** – ang mga transaksyon ay hinahati sa maramihang piraso at ipinapakilala ang blinding factors sa koleksyon ng mga pirasong iyon, kaya ang mga halaga ng mga piraso at ang ibang parametro ng transaksyon ay hindi malalaman;
- ***Dandelion++ Protocol*** – tinatakpan ang mga digital na landas ng transaksyon galing sa IP address ng nagpapadala;
- ***CoinJoin*** – pinagsasama-sama ang mga transaksyon sa loob ng mga bundles upang itago ang relasyon sa pagitan ng magkatransaksyon partido.

[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

All Epic Cash blocks contain:



Merkle Trees of transaction inputs; **Merkle Trees of transaction outputs and rangeproofs;** **A list of excess values and signatures.**

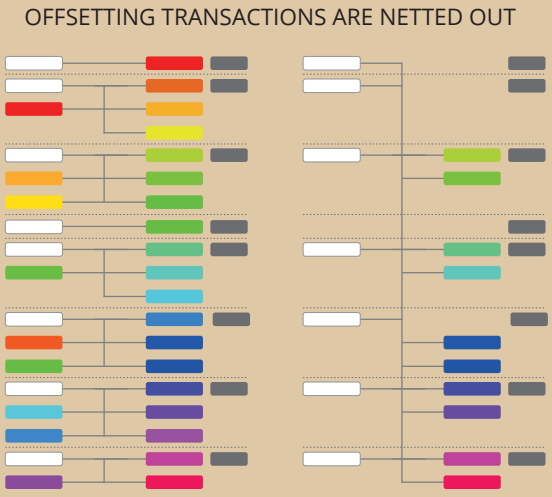
In Figures 2 and 3, adapted from Andrew Poelstra's presentations[10], we can see newly mined Epic represented as the white input cells. Identically colored cells represent outputs with corresponding spent inputs. With the Cut-Through process, inputs and matching spent outputs are removed to free up space within the block, which reduces the amount of data that needs to be stored on the blockchain. While the transactions are omitted from the ledger, the remaining excess kernels (a mere 100 bytes) permanently document that the transactions took place.

As blocks continue to be created, MimbleWimble applies Cut-Through across blocks, so that over the long run all that remains are the block headers (approximately 250 bytes), unspent transactions, and transaction kernels (approximately 100 bytes). Grin, the second MimbleWimble implementation to be launched, showed that a MimbleWimble chain with a similar number of transactions to the Bitcoin chain would be nearly 10% of the size of Bitcoin's chain[11]. Furthermore, the size of a node will be "on the order of a few GB for a Bitcoin-sized chain, and potentially optimizable to a few hundred megabytes."[12]

This stands in marked contrast to Bitcoin, where the entire blockchain must be stored by each node. Over time, as the space efficiency of the Epic Cash blockchain grows relative to the Bitcoin blockchain, so too will the cost efficiencies relative to the participation of nodes in the Epic Cash network. Lower barriers to participate helps ensure crucial resilience at the node layer of network design.

Through its implementation of MimbleWimble and application of chain pruning with the Cut-Through process, the Epic Cash blockchain offers scalability in a way often overlooked by the cryptocurrency community. It is one that captures the essence of Bitcoin and like-minded projects: decentralization. Regardless of how many transactions per second a coin might be able to process, what good is it if it can't be sustained by a broad and diverse network? If memory requirements are such that validation ultimately gravitates towards strong mining conglomerates, then all of the cryptocurrency community's efforts to create a decentralized ecosystem are obviated. To provide for additional throughput, a Lightning-style Layer 2 implementation is planned as a short-term objective in the Epic Cash development roadmap.

Figure 3: MimbleWimble transactions before and after Cut-Through.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&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. Monetary Policy

The monetary policy of Epic Cash and Bitcoin are very similar. Epic Cash circulating supply first expands rapidly and then synchronizes with the circulating supply of Bitcoin in 2028. It increases thereafter at a declining rate until reaching a maximum supply of 21 million Epic in 2140. Epic Cash has the qualities to become a safe store of long-term value because the circulating supply is known at any point along its emission lifecycle and culminates in a fixed maximum supply. The Epic Cash monetary policy is characterized by the following four features:

- Rapid emission over the first nine years of its lifespan, during which 20,343,750 Epic (96.875% of the total supply) are to be mined. The exact emission rates are outlined in the Emission Schedule section of this paper;
- A maximum supply of 21 million Epic will be reached in year 2140, at approximately the same time as when Bitcoin reaches a maximum supply of 21 million units;
- The Epic circulating supply and emission rate synchronize with those of Bitcoin on the Epic Singularity around May 24, 2028. Following the Singularity, the emission rate decreases at an increasing rate, while the circulating supply grows at a decreasing rate;
- Epic has an 8 decimal divisibility structure, such that: 1 Epic is equal to 100,000,000 freeman (just as 1 Bitcoin is equal to 100,000,000 satoshi).

The Epic Cash monetary policy is modeled after Bitcoin's for the following reasons:

- Agreement with the economic fundamentals of Bitcoin, namely that scarcity and predictability of circulating supply underlie its strong store of value properties;
- The public is already familiar with Bitcoin's model and its proven track record over the last ten years since its inception. By approximately synchronizing with Bitcoin's circulating supply, and mirroring Bitcoin's maximum supply and divisibility structure, Epic takes the path of least resistance towards mass adoption.

VII. Mining

The Epic Cash blockchain pursues decentralization by welcoming a wide variety of computation hardware. Epic mining is initially available to CPUs, GPUs, and ASICs, using three respective hashing algorithms: RandomX, ProgPow, and CuckATOO31+. Algorithms can be trivially hot-swapped without compromising the integrity of the chain.

1 RandomX and CPUs

RandomX is a Proof-of-Work (PoW) algorithm optimized for general purpose CPUs. It uses randomized program executions with several memory-hard techniques to achieve the following goals:

- Prevention of the development of single-chip ASICs;
- Minimize the efficiency advantage of specialized hardware over general purpose CPUs.

Mining Epic with CPUs requires a contiguous allocation of 2 GB of physical RAM, 16 KB of L1 cache, 256 KB of L2 cache, and 2 MB of L3 cache per mining thread[13]. Windows 10 devices require 8 GB or more RAM. It is not inconceivable that one day in the not-too-distant future mobile phones could become viable mining nodes. Early CPU integration in the Epic Cash mining network is an excellent opportunity for many with only modest computing means to earn block rewards by helping to secure the Epic Cash network.

2 ProgPow and GPUs

Programmatic Proof-of-Work (ProgPow) is an algorithm that depends on memory bandwidth and core computation of randomized math sequences, which take advantage of many of a GPU's computing features and thereby efficiently capture the total energy cost of the hardware. As ProgPow is specifically designed to take full advantage of commodity GPUs, it is both difficult and expensive to achieve significantly higher efficiencies through specialized hardware. As such, the ProgPow algorithm mitigates incentives for large ASIC pools to outcompete GPUs, as is often seen with many other PoW algorithms, such as Bitcoin's SHA-256. GPUs, although not as prevalent as CPUs, are still commonly available. With technological development driven by powerhouses, Nvidia and AMD, GPUs are able to parallel process many multiples of mining solutions above CPUs on a per unit basis. It is due to this combination of ubiquity and high processing power that GPUs will provide the backbone to much of the mining activity during the initial eras, as indicated in Table 2.

3 CuckATOO+31 and ASICs

CuckATOO31+ is an ASIC friendly permutation of the Cuckoo Cycle algorithm developed by Dutch computer scientist, John Tromp. A relative of the ASIC resistant CuckARoo29, CuckATOO31+ generates random bipartite graphs and presents miners with the task of finding a loop of given length 'N' passing through the vertices of that graph.

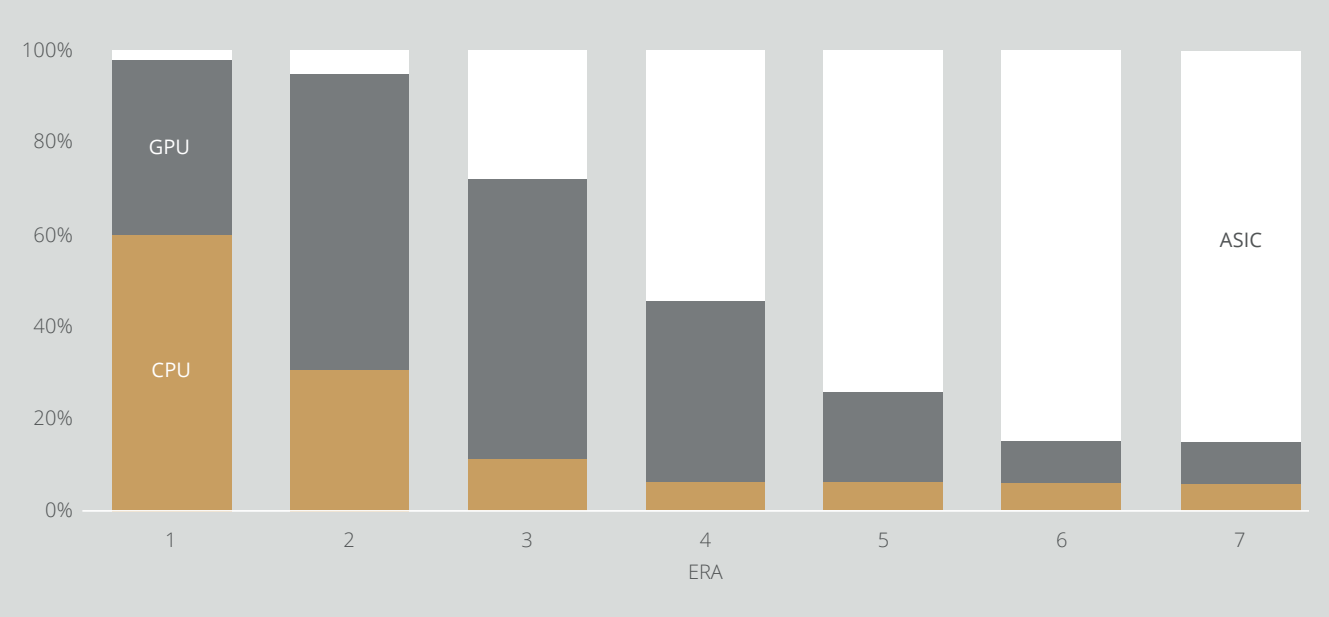
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

This is a memory bound task, meaning the solution time is bound by memory bandwidth rather than raw processor or GPU speed. As a result, the Cuckoo Cycle algorithms produce less heat and consume significantly less energy than traditional PoW algorithms. The ASIC friendly CuckATOO31+ allows efficiency improvements over GPUs by using hundreds of MB of SRAM while remaining bottlenecked by memory I/O[14]. Ultimately, ASICs offer the greatest potential economies of scale of the three mining options. In the interest of inclusivity, however, though they are allocated a small portion of mining rewards relative to CPUs and GPUs early on, eventually ASICs assume a majority stake of the mined block rewards, on the assumption there will be a competitive ecosystem of device manufacturers for CuckATOO31+.

Table 2: Mining reward allotments. Subject to revision. Allotments will be directed to achieve maximum decentralization and consistent with the long term interests of the network.

Era	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%

Figure 5: Mining reward allotments for each era according to Table 2. Subject to revision.



[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 Mining Contributions

Starting at the Epic Genesis (2019) and concluding at the Epic Singularity (2028), during the mining process, there is an allocation of Epic that is redirected, as mining contributions, towards the EPIC Blockchain Foundation.

The EPIC Blockchain Foundation is dedicated to technical development and promoting awareness and utility of the Epic Cash project during the early years of its inception, by creating marketing activities and developing partnerships within the financial technology industry.

After the Singularity, the EPIC Foundation's role will be assumed by the EPIC Distributed Autonomous Corporation (EDAC), that will be developed by the foundation prior to the handover.

The EPIC Blockchain Foundation is funded by a percentage of mining rewards, deducted from block rewards, according to the following annual rates:

Table 3: Annual rates for Foundation mining contributions as percentage of mining rewards.

Year	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% of Mining Rewards	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Conclusion

Epic aims to be recognized as 'decentralized digital silver', a medium of exchange counterpart to Bitcoin's recognized position as decentralized digital gold. By reintroducing lost fungibility on a much more energy-efficient and ecologically-friendly hardware backbone, Epic Cash tilts the balance of power back in favor of individual users, in stark contrast with recent centralizing trends. The combination of Bitcoin economics, game theory, and proven proof-of-work formula with the best of contemporary blockchain technology results in a trustless, immutable, and decentralized currency (Epic) that is scalable, fungible, and that protects the privacy of its users. The Epic Cash blockchain is open, public, borderless, and censorship-resistant. It preserves the privacy and wealth of its users and rewards those who deploy their hardware in support of the network via mining. Every Epic is mined into existence via proof of work. Supply begins at zero and the network is considered fair launched, with a functional testnet currently running.

Epic Cash Key Facts:

- **Mining begins August 1st, 2019.**
- **The Epic Cash blockchain is based on MimbleWimble.**

  Defining features of the protocol are:

  1. **Cut-Through** – the removal of redundant information from the blockchain to promote space efficiency, encourage wide scale participation in network validation, and steward decentralization;
  2. ***CoinJoin*** – the bundling of transactions within a block to ensure the fungibility of the Epic cryptocurrency;
  3. ***Dandelion++ Protocol*** – the propagation of transactions by communicating across intertwined channels, and diffusing across a broad network of nodes, severing connections between transactions and their origin;
  4. **No Wallet Addresses** – the use of a grand multisignature to generate single-use private keys for transacting parties, eliminating the need for wallet addresses entirely.

- **The Epic Cash monetary policy** is designed to synchronize the Epic circulating supply with Bitcoin's circulating supply in roughly nine years, and reach the same maximum supply of 21 million units at the same time as Bitcoin, in the year 2140. This decreasingly inflationary policy guarantees transparency, predictability of supply, and scarcity, fostering the security of long-term value storage.

- **Mining** which incorporates CPUs, GPUs, and ASICs via corresponding RandomX, ProgPow, and CuckAToo31+ algorithms, to facilitate mass adoption and network efficacy.

IX. Technical Specifications

Project Name: Epic Cash
Currency Name: Epic
Block Time: 60 seconds
Block Size: 1 MB
Starting Supply: 0
Final Supply: 21,000,000
Genesis Block: August 1, 2019
Consensus: RandomX (CPUs), ProgPow (GPUs) and CuckATOO31+ (ASICs)

Links:

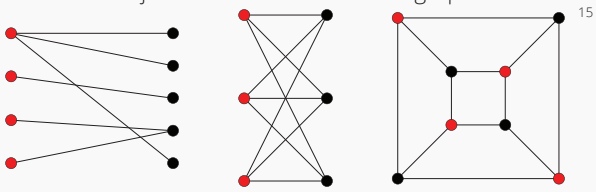
www.epic.tech

t.me/EpicCash – Telegram

X. Glossary

ASIC Application Specific Integrated Circuits; chips that are designed for a singular purpose

Bipartite Graph a set of graph vertices decomposed into two disjoint sets such that no two graph vertices within the same set are adjacent.



Blinding Factor a random element introduced into a digital message to facilitate encryption; a shared secret between the two parties that encrypts the inputs and outputs in that specific transaction as well as the transacting parties' public and private keys[16].

Block Reward the new Epic distributed by the network as rewards for computations performed to verify the transactions within a new block.

Cache a hardware or software component that stores data so that future requests for that data can be served faster.

Circulating Supply the amount of Epic in existence at a given point in time.

CPU Central Processing Unit: computer component responsible for interpreting and executing most of the commands from the computer's other hardware and software.

Cut-Through a MimbleWimble blockchain process whereby inputs and matching spent outputs are removed to free up space within the block, reducing the amount of data needed to be stored on the blockchain.

Decentralization the state of dispersion of a network's operations and governance.

Emission the creation of new Epic earned by miners in block rewards. Epic is created every 60 seconds as transactions are confirmed into the blockchain.

Epic Singularity the point at which Epic's circulating supply synchronizes with Bitcoin's circulating supply (May 2028).

Excess (MimbleWimble) the difference between outputs and inputs, plus signatures (for authentication and to prove non-inflation).

Fungibility the property of a good or commodity whereby individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.

Genesis (Event) the mining of the first Epic block and official inception of the blockchain.

GPU Graphics Processing Unit: A unit containing a programmable logic chip (processor) specialized for display functions. Consumer GPUs can be well-suited for cryptocurrency mining.

Halving (for Bitcoin) occurs every 4 years. The rate of supply decreases by 50% after each halving event.

Hash a value computed from a base input number using a hashing function.

Hashing Algorithm (function) mathematical algorithm that maps data of arbitrary size to a hash of a fixed size used for generating and verifying digital signatures, message authentication codes (MACs), and other forms of authentication.

Homomorphic Encryption a method of performing calculations on encrypted information without decrypting it first. (in

Immutability programming) the state in which an object cannot be modified after its creation.

Input (MimbleWimble) the component of a MimbleWimble transaction representing the sending party of the transaction; created from outputs of previous transactions.

I/O input/output; the communication between an information processing system, such as a computer, and the outside world, possibly a human or another information processing system.

[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/

Maximum Supply	the amount of Epic to be reached at which point the circulating supply will not increase thereafter (21,000,000 Epic).
Memory-Hard	the use of a lot of RAM to preclude simultaneous connections running attempts in parallel. Memory-hard functions are algorithms which have computation times primarily decided by available memory to hold data. Also known as memory-bound functions.
Merkle Tree	a data structure used in computer science applications. In blockchains, Merkle trees allow for efficient and secure verification of the contents in large data structures.
MimbleWimble	a protocol put forth by a pseudonymous contributor, going by the moniker Tom Elvis Jedusor, in a Bitcoin developers' chatroom.
Multisignature	a digital signature scheme which allows a group of users to sign a single document. Usually, a multisignature algorithm produces a joint signature that is more compact than a collection of distinct signatures from all users[17].
Node	a computer that connects to a blockchain network and branches out to other nodes within the network to distribute information about transactions and blocks, in a peer-to-peer manner.
One Way Aggregate Signature (OWAS)	a transaction signature composed of many signatures that is encrypted in a way so that it is very difficult to compute the individual signatures that are part of the aggregate.
Output (MimbleWimble)	the component of a MimbleWimble transaction representing the receipt of the transaction; used as inputs for subsequent transactions.
Pedersen Commitment Scheme	a cryptographic primitive that allows a prover to commit to a chosen value without revealing any information about it and without the prover being able to rescind committing to the value.
Private Key	a private key is a tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format.
Proof of Work (PoW)	a piece of data which is difficult (costly and time consuming) to produce, but easy for others to verify, and which satisfies certain requirements. Proofs of Work are often used in cryptocurrency block generation.
Public Key	a public key is created in public key encryption cryptography that uses asymmetric-key encryption algorithms. Public keys are used to convert a message into an unreadable format.
RAM (Random Access Memory)	fast-access data storage chips in a computing device where the operating system (OS), application programs and data in current use are kept so they can be quickly reached by the device's processor.
Rangeproof	a commitment validation which verifies that the sum of a transaction inputs is greater than the sum of the transaction outputs and that all the transaction values are positive. Rangeproofs ensure that the monetary supply hasn't been tampered with.
(Digital) Signature	a standard part of a blockchain protocol, mainly used for securing transactions and blocks of transactions, transferral of information, contract management and any other cases where detecting and preventing any external tampering is important. They provide three advantages of storing and transferring information on the blockchain: • They reveal if the data being sent has been tampered with; • Verifies the participation of a particular party in the transaction; • Can be legally binding.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) that retains data bits in its memory as long as power is being supplied.
Throughput	the measure of transactions per second that can be performed by a given cryptocurrency protocol.
Trustlessness	the quality of a cryptocurrency network to adhere to the rules of a protocol without enforcement by a central party.

[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