Freeman Family

July 4, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

A Peer-to-Peer Electronic Cash System

STORE OF VALUE + MEDIUM OF EXCHANGE + UNIT OF ACCOUNT

1.7 billion adults have no access to the global financial system, while another 1.3 billion are underserved. Epic Cash unlocks human potential by connecting individuals to the global market. Fast, virtually free to use, and open to all.

Version 7.1b

Contents

I. Abstract

Epic Cash is the final point in the journey toward true P2P internet cash, the cornerstone of a private financial system. The Epic currency aims to become the world's most effective privacy-protecting form of digital money. In order to fulfill that goal, it satisfies the three principal functions of money:

1. **Store of Value** – can be saved, retrieved, and exchanged at a later time, and of predictable value when retrieved;
2. **Medium of Exchange** – anything accepted as representing a standard of value and exchangeable for goods or services;
3. **Unit of Account** – the unit by which the value of a thing is accounted for and compared.

	$ USD	BTC	EPIC
Store of Value	✗	✓	✓
Medium of Exchange	✓	✗	✓
Unit of Account	✓	✗	✓

In 2009 Bitcoin emerged as the first blockchain-based digital currency, and with it three defining characteristics against which other cryptocurrencies are evaluated:

- **Trustlessness** – nobody is required to trust any centralized entity or counterparty in order for the network to function;
- **Immutability** – transactions cannot be undone;
  a. It should be highly improbable or difficult to rewrite history;
  b. It should be impossible for anyone but the owner of a private key to move funds associated with that private key;
  c. All transactions are recorded in the blockchain.
- **Decentralization** – "Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural point of failure)..."[1].

Bitcoin blazed new trails technologically while adhering to time-tested fundamentals in the structure of its monetary policy. Bitcoin's success is strongly related to its limited supply combined with trustless, immutable, and decentralized blockchain. Epic Cash emulates Bitcoin's monetary policy of decreasing inflation and limited supply to ensure Epic currency can serve as an effective store of value.

Despite Bitcoin's success, certain shortcomings have been revealed since its inception 10 years ago. Other projects have tried to overcome these shortcomings and we have investigated the best of these to use as our starting point. We decided upon utilizing the Grin codebase and the excellent work of several other projects to help us perfect on the hard-won accomplishments and discovered faults of Epic Cash's predecessors. Epic Cash possesses the key qualities to be an ideal currency:

- **Fungibility** – The value of a given unit of Epic must always be equal to another unit of Epic, just as one Yen or Yuan is always equal to and replaceable with another Yen or Yuan. The achievement of fungibility in large part hinges on privacy.
- **Privacy** – The Epic Cash blockchain safeguards the anonymity of Epic holders and users by protecting the details of transactions from third parties, and is designed to be both untraceable and invisible to surveillance.
- **Scalability** – Epic Cash maintains a space efficient blockchain, upon which new nodes can be easily established without resource-intensive equipment. The Epic Cash blockchain is capable of at least twice the throughput of Bitcoin.
- **Speed** – The Epic Cash transactions are smooth, continuous and are executed much faster than in previous generations of blockchain technology. While Bitcoin requires six 10-minute blocks to achieve complete transaction confirmation, Epic transactions occur within a single block confirmation as soon as a 1-minute block has been mined.

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

II. Privacy

The modern day use of money can be understood as the collective transference of units of account between people and institutions. The landscape of money at any given point in time can be mapped by answering the following questions:

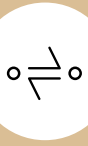
1. *Who is holding it, and how much are they holding?*
2. *Who is transacting with whom, and for how much?*

For traditional fiat currencies, and indeed Bitcoin as well, we can answer those questions. In so doing, much can be revealed about people's lives, such as consumption patterns, ownership, and transactional counterparties. Fairly accurate conclusions can be drawn about an individual's interests and intentions by tracing transfers of value. Without privacy, transaction data can be dangerous information in the hands of predatory third parties.

The past decade's use of cryptocurrency shows a continuum of "privacy" in varying blockchain implementations. The privacy scale, should one be considered, ranges from open and notorious on one end to anonymous on the other. As privacy erodes, one essential cornerstone of cryptocurrency, trustlessness, degrades. As evidenced by the success of Bitcoin blockchain analysis services, Bitcoin is situated more towards the notoriously transparent end of the privacy spectrum. Users must increasingly take steps to ensure they don't inadvertently transact in tainted Bitcoin. The Epic Cash solution swings the needle towards anonymous and restores this essential property by ensuring that both the privacy of the individual and privacy of transactions are engineered into the system at a fundamental level.

Privacy of Identity

Privacy of Transaction



Privacy of Identity

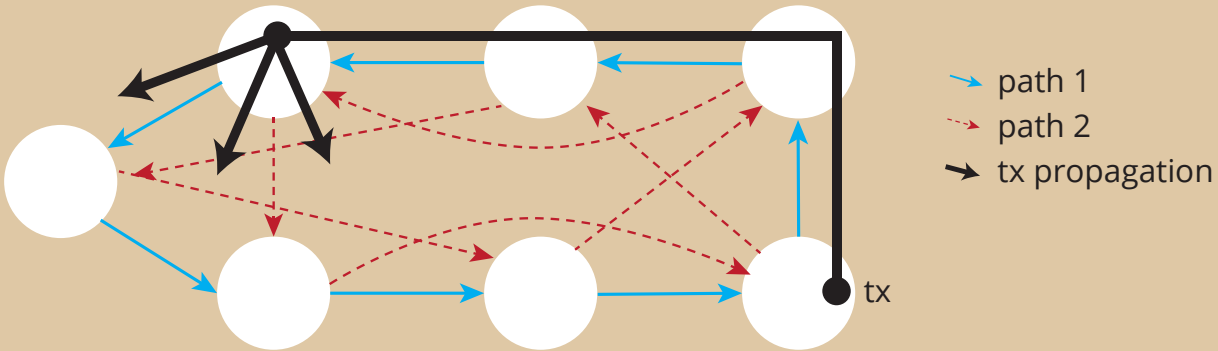
Most cryptocurrencies like Bitcoin are stored in wallets whose addresses refer to public keys derived from a wallet's private keys. These addresses can be thought of as locators of one's private vault in the digital world. The Epic Cash blockchain eliminates addresses entirely and instead applies one grand multisignature from which all public and private keys are generated on a single-use basis.

Because Bitcoin wallet addresses are a vault's locator in the digital world, that wallet can be traced to an owner's Internet Protocol (IP) address, which anchors the owner to a computer at a unique location at a given point in time. Simply explained: when a Bitcoin transaction takes place, the transaction is broadcast from a communication hub called a 'node' and then propagated to other nodes called 'peers'. That information then quickly spreads to each of those nodes' peers consecutively across the entire network. This process is aptly named the "Gossip Protocol". Quite simply, each Bitcoin has a visible online position and a physical location where it, or rather the Bitcoin owner, can be found. As journalist Grace Caffyn noted, Bitcoin is "no more secret than a Google search from a home internet connection."[2]

In addition to eliminating wallet addresses, the Epic Cash blockchain secures privacy of identity by ensuring IP addresses can't be traced. It does this through the integration of the ***Dandelion++ Protocol***. Improving upon its predecessor, the original ***Dandelion Protocol***, the ***Dandelion++ Protocol*** is a result of seven researchers' continued work to combat deanonymization attacks on the blockchain. Through ***Dandelion++***, transactions are passed over random intertwined paths, or 'cables', and then suddenly diffused to a large network of nodes, like the pods of a Dandelion flower when blown from their stem (Figure 1). This makes it nearly impossible to trace transactions back to their origin, and thus their originating IP addresses.

Figure 1: Anonymizing transactions with the *Dandelion++ Protocol.*

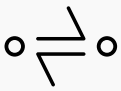
Dandelion++ forwards messages over one of two intertwined paths on a 4-regular graph, then broadcasts using diffusion. In the figure, the transaction propagates over the blue solid path[3]. This process makes it extremely difficult to trace transactions back to their source, thereby preserving privacy.



[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

Privacy of Transaction



The Epic Cash blockchain assures transaction privacy by obscuring amounts and the sender-receiver relationship of a transaction. This is achieved through the application of ideas familiar from ***Confidential Transactions (CT)***[4] and ***CoinJoin***[5], methods in large part developed by Gregory Maxwell (Bitcoin Core developer, Co-Founder and CTO of Blockstream).

CT, originally created by Adam Back and later refined by Maxwell, works by breaking transactions into smaller parts through homomorphic encryption, a method of performing calculations on encrypted information without decrypting it first to preserve privacy. Once divided up, observers cannot see the actual amounts of the transactions because of blinding factors, a system that throws random numbers into the mix of transaction fragments to conceal the values of those fragments. Ultimately, only transacting parties know the value of an exchange, while the transaction is verified by the network through confirmation that the sum of the output values equals the sum of the input values, and the sum of the output blinding factors equals the sum of the input blinding factors.

To further complicate the task of prying eyes, all Epic Cash transactions are cloaked with ***CT*** and then mixed together to hide the connections between transacting parties. This is done through Maxwell's second concept, ***CoinJoin***.

To illustrate ***CoinJoin*** simplistically, imagine that A, B and C are sending Epic to X, Y and Z, respectively. Sent through the ***CoinJoin*** medium, all that is known is that A, B and C are sending and X, Y and Z are receiving, while the transaction amounts remain invisible. The ***CoinJoin*** system is fundamental to Epic Cash through One-Way Aggregate Signatures (OWAS), which combine all transactions inside a block into a single transaction.

Privacy: Summary

The Epic Cash blockchain protects the privacy of individuals and their transactions by:

- **Eliminating wallet addresses – There are no location identifiers to digital vaults within the blockchain. Transactions are constructed directly person-to-person on a wallet-to-wallet basis;**
- ***Dandelion++ Protocol* – obscures the digital pathways of a transaction from the transaction sender's IP address;**
- ***Confidential Transactions* – divide transactions into multiple pieces and introduce blinding factors into the collection of those pieces, so that the values of the pieces and other transaction parameters cannot be known;**
- ***CoinJoin* – combines transactions into bundles to mask the relationships between transacting parties.**

[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. Fungibility

Charlie Lee, the creator of Litecoin, stated that fungibility was the only property of sound money missing from Bitcoin and Litecoin, admitting that privacy and fungibility were the next battlegrounds for those coins[6]. Andreas Antonopoulos, one of the world's foremost blockchain experts, claimed that "...tainted coins are destructive. If you break fungibility and privacy, you break the currency."[7]

Fungibility is the property of a set of goods or assets that ensures the individual units of that set are of equal value and are interchangeable. It is what differentiates the earliest forms of currency from their preceding systems of barter. Without confidence in the fungibility of money, that money rapidly loses its utility. As will be illustrated below, the fungibility of most cryptocurrencies is uncertain, whereas Epic Cash's privacy architecture ensures it is impervious to the same threats.

Most cryptocurrencies similar to Bitcoin, by the nature of the transparent blockchains on which they exist, can be verifiably traced through every wallet in which they were kept. Private third parties and governments alike monitor the Bitcoin blockchain with increasingly sophisticated means to quickly identify coins used in previous activities. This naturally leads to concerns that tainted coins might someday be banned from transactions, leaving their subsequent good-faith holders at a loss.

On March 19, 2018, the U.S. Office of Foreign Asset Control (OFAC) announced it was considering including digital currency addresses to the list of Specially Designated Nationals (SDNs), which are entities with whom U.S. persons or businesses are forbidden to transact. Even more troubling, the OFAC has not ruled out the inclusion of addresses currently holding tainted coins on to the SDN list, which would effectively place innocent owners of tainted cryptocurrency on a criminal blacklist due to the affiliation of the tainted coins owned. This has led New York University legal professor, Andrew Hinkes, to quip, "kiss fungibility goodbye," and that the public should expect "a premium on freshly minted coins, or traced clean coins..."[8].

With these developments in mind, it's not difficult to imagine an upheaval in the crypto market and the suffering, or even extinction, of many well-established cryptocurrencies. However, Epic is one of the few cryptocurrencies that avoids this problem entirely due to the strong privacy features previously described in this paper. By removing the link between identity and ownership, and the relationship between transacting parties, Epic can never be affiliated to a person or an activity. As such, the value of Epic remains independent of its users and provides high degrees of privacy and security that cannot be easily manipulated by malicious actors in criminal, financial, or political arenas.

> **"...TAINTED COINS ARE DESTRUCTIVE. IF YOU BREAK FUNGIBILITY AND PRIVACY, YOU BREAK THE CURRENCY."**
>
> **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. Scalability

Epic Cash is a MimbleWimble blockchain implementation that yields advances in scalability as a result of space efficient design that sheds redundant transaction data. The Cut-Through functionality responsible for this assures that the blockchain grows more space efficient over time unlike most cryptocurrencies, including Bitcoin, and that new nodes can be created with minimal investments in memory and computing power. By remaining space efficient, it capacitates a widely dispersed network and fosters decentralization. Furthermore, while each Bitcoin node must store the entire chain, Epic Cash nodes are able to contribute to network security based on a small subset of blocks.

Most cryptocurrencies require indefinite storage of all transaction data on their blockchains. The Bitcoin chain currently gains 0.1353 GB of memory each day, while Ethereum's chain increases at an even faster rate of 0.2719 GB a day. If Bitcoin's chain continues to grow at its current rate, it will eventually reach an approximate 6 TB in size by the time its last reward block is mined in the year 2140. Ethereum will surpass 10 TB by that date[9]. In most blockchains without MimbleWimble, transactions must be verified by nodes all around the world. As data increases, so does the burden on each node. Even at only 200 GB (the approximate size of the current Bitcoin chain), synchronizing the data requires a stable network and high-speed disk read and write capability.

Consequently, mining has become increasingly centralized among large pools leveraging costly computing resources. **If the entire blockchain history of Bitcoin were to be stored on the Epic Cash blockchain instead, it would fit into nearly 90% less space.** Smaller is faster because each transaction requires less time to transmit and secure.

MimbleWimble solves this storage dilemma with an innovative method of block pruning, referred to as 'Cut-Through'. In order to understand how Cut-Through works, it's best to first look at how transactions and blocks are composed within a MimbleWimble blockchain.

Inputs:

References to old outputs;

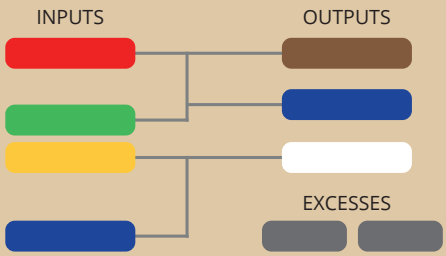
Outputs:

Confidential Transaction outputs and **rangeproofs**;

Excess:

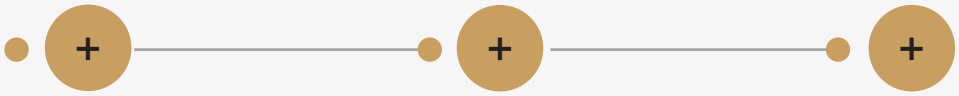
The difference between outputs and inputs, plus **signatures** (for authentication and to prove non-inflation).

Figure 2:
MimbleWimble transaction parts.



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

All Epic Cash blocks contain:



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

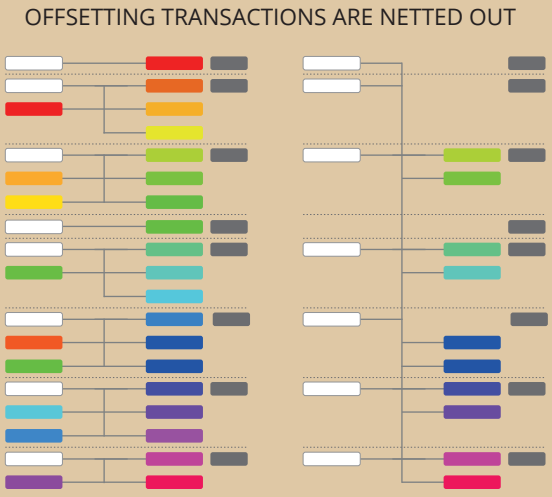
In Figures 2 and 3, adapted from Andrew Poelstra's presentations[10], we can see newly mined Epic represented as the white input cells. Identically colored cells represent outputs with corresponding spent inputs. With the Cut-Through process, inputs and matching spent outputs are removed to free up space 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;
- 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;
- 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;
- 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.

VI. Emission Schedule

Epic Cash has a total of 33 mining eras, each defined by decreases in block rewards, relative to their preceding era. The Epic Genesis, the date on which Epic block #1 is mined, takes place on August 1, 2019. Blocks are mined at one per minute. The first five eras produce nearly 97% of the Epic maximum supply, matching 20 years of Bitcoin emissions in approximately nine years. This can be thought of as a chance to 'turn back the clock' for those who missed out on the spectacular rise of Bitcoin.

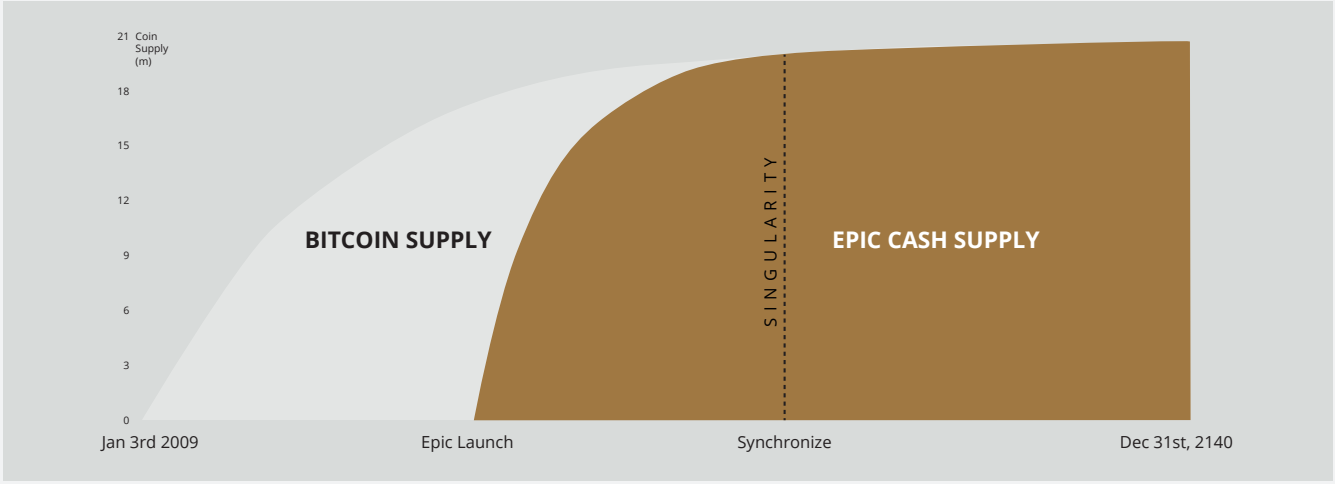
The emission schedule in table 1 outlines the start and end dates of the first seven mining eras, their corresponding block rewards, and the ensuing circulating supplies for each era. The eras 8 to 33 are not included in the table for brevity's sake. For those eras, it should suffice to understand that each subsequent era will have a block reward that is half the amount of the reward of the preceding era, exactly as in Bitcoin. The amount of Epic emitted during each of these eras will be the sum of block rewards within the 4-year era (approximately 1460 days).

At the Epic Singularity (2028), the Epic circulating supply intersects the number of Bitcoin's circulating supply, at which point Epic Cash adopts the Bitcoin block reward and halving pattern, which sees block rewards decrease by half every four years. The only exception is that Epic blocks continue to be mined at a rate of one each minute, versus Bitcoin's rate of one block every ten minutes. By doing this, the Epic circulating supply maintains approximate parity with Bitcoin's circulating supply for the remainder of their existence.

Table 1: Emission schedule for the first seven mining eras. Dates are close approximations.

Era	1	2	3	4	5	SINGULARITY	6	7
Block Reward	16	8	4	2	1		0.15625	0.078125
Start Date	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
End Date	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Length (in days)	334	470	601	800	1019		1460	1460
Starting Supply	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
End Supply	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% of Maximum Supply	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figure 4: Epic and Bitcoin emission schedules.



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.

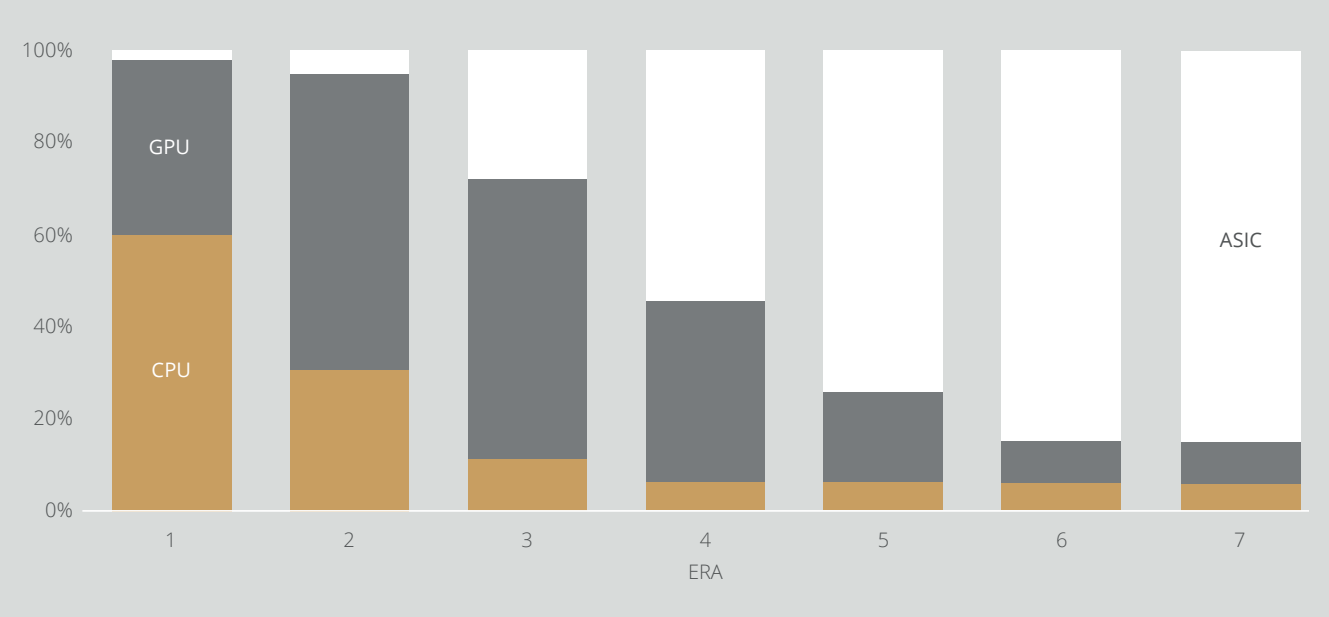
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

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:

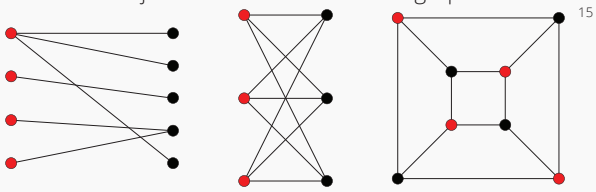
www.epic.tech

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