SafeCoin

An evolving dedication to freedom and liberty through decentralized security

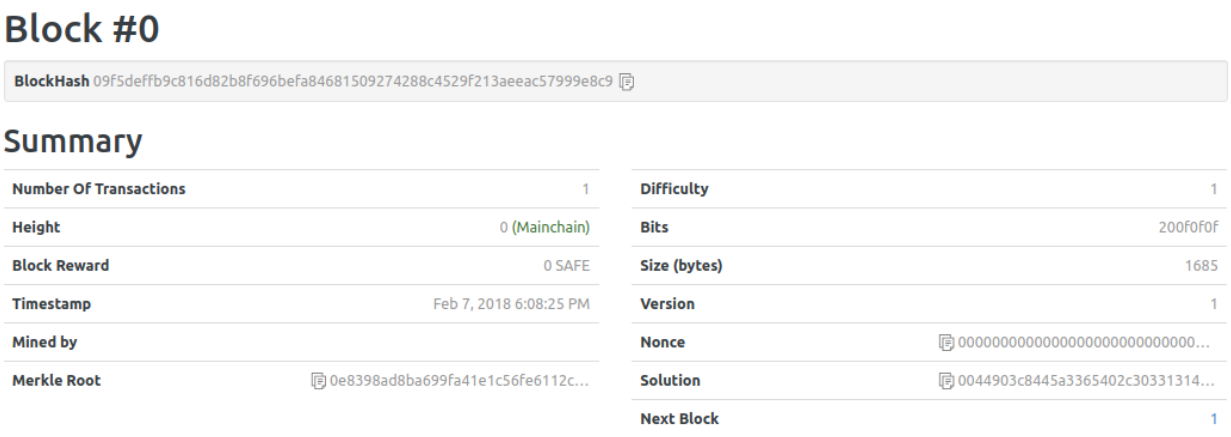
Table of Contents

Introduction

On the Seventh of February 2018, the world lost a champion and pioneer of Digital Rights, John Perry Barlow. A gifted lyricist, John brought the world some of the finest music of his generation. As a digital age approached, John was able to transcend his connection with humanity to a new landscape. John became a world-renowned pioneer in digital rights and freedoms at the very dawn of the internet itself. Much of the digital freedoms we take for granted today are a direct result of his tireless work and dedication.

In honor of John Perry Barlow's passing and on this same day, the Safecoin Genesis block was created:

```
psztimestmp("CNN 2018/02/07 Internet rights advocate John Perry Barlow dies");
```



Block #0

BlockHash 09f5deffb9c816d82b8f696befa84681509274288c4529f213aeeac57999e8c9

Summary

Number Of Transactions	1	**Difficulty**	1
Height	0 (Mainchain)	**Bits**	200f0f0f
Block Reward	0 SAFE	**Size (bytes)**	1685
Timestamp	Feb 7, 2018 6:08:25 PM	**Version**	1
Mined by		**Nonce**	00000000000000000000000000000...
Merkle Root	0e8398ad8ba699fa41e1c56fe6112c...	**Solution**	0044903c8445a3365402c30331314...
		Next Block	1

[4]

In his own words: *"The future's here, we are it, we are on our own."*

From that moment on, a growing passionate community at the Safecoin project has done everything we can to grow and promote freedom and liberty through decentralized security. We will continue to evolve both our technology and our understanding of what humanity can become in a decentralized world and economy.

The development of SafeCoin builds upon proven cryptocurrency code and ideals with a goal of making a safe and global cryptocurrency ecosystem that can be used by individuals, businesses, and governments. SafeCoin begins with the belief that liberty, truth, and freedom in a digital age are built directly upon the

foundations of strong decentralized security and privacy. For that, we are very thankful for the incredible contributions from which our work is built from. Komodo [2], for its dedicated and groundbreaking focus on security and continuous advancement. Zcash [3], for bringing the world's first provable private blockchain transactions. Last and definitely not least, Bitcoin [1] for revolutionizing our generation with blockchain and decentralized store of value.

SafeCoin is a community driven project with a growing and dedicated team of talented and passionate individuals. We are aligned in the vision of building a safe, secure and decentralized foundation capable of realizing the full potential of what blockchain has to offer humanity and the environment we depend upon.

A fundamental value in our project and our community is that we are stronger together. Blockchain is for everyone. We support everyone who contributes to blockchain, and we believe that anyone with a dream to make this world better with blockchain should have a chance to realize that dream. We do not compete with blockchains. We compete with fiat. At all possible turns we choose to work with other blockchain projects to make them stronger. We work with businesses to give them the tools to prosper in a decentralized multifaceted economy. We work with individuals who strive to see their innovations realized. This philosophy is in every interaction we have, every feature we add, every goal we set, and in all the code we write. It is never enough to have a single point of security. We believe in a diverse thriving network of innovation that allows creativity and inspiration to be realized in a store of value anywhere in the world at any time. We are working to foster a stronger, safer blockchain community through cooperation, collaboration, and innovative networking solutions that provide the security for dreams to be realized.

"We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth."

-John Perry Barlow - A declaration for the independence of cyberspace[6]

Challenges

To improve blockchain technology, we must look at the challenges that the current fiat currency and centralized banking options present to the end-user, and what can be improved over Bitcoin and subsequent cryptocurrencies.

- Security
  - Cryptocurrencies, while decentralized, are prone to single points of failure in their consensus mechanisms. Most notably, malicious double-spending exploits inherent in proof of work projects.
  - Most cryptocurrencies suffer from at least one form of centralized dominance, which can be regional, investor based, or founder based. As such, any single blockchain no matter how large may be prone to collusion [8]

    - Banks have security that is good at *protecting their assets,* but they don't protect their customers. Banks thrive on fees and customer mistakes, so the customer does not have security *from* the bank.
    - Cryptocurrencies have suffered from security breaches regularly since Bitcoin was released. The loss, theft, and false mining of millions of dollars' worth of cryptocurrency have occurred.
- Privacy
    - Privacy is a growing concern as our world and lives become more interconnected. Banks, governments, and corporations all trade customer data as a commodity and our habits and wealth (or lack of) are known and marketed to.
    - Much of our personal information, and maybe even passwords, are potentially available online, and many people aren't aware of this.
- Sustainability
    - Existing methods of Cross-chain linking have an expense
        - Because of the expense, cross-chain linking has numerous limitations
- Accessibility and ease of use
    - There is still a user-interface barrier to most cryptocurrencies. A project must have useful and intuitive wallets, including mobile wallets, without a security tradeoff.
- Inflation and emission rates can keep a coin from being usable as a store of value.

SafeCoin was developed to meet the needs of users and has addressed as many of the challenges as possible.

Privacy & Anonymity

"When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl."

-an anonymous quote (of course), widely attributed to John Perry Barlow.

Translates to: "When cryptography is outlawed, only outlaws will have privacy."

Often these terms are used interchangeably, but they differ significantly. A transaction is "anonymous" if no one knows who you are. A transaction is "private" if what you purchased, and for what amount, are unknown. Credit card transactions are not anonymous nor private. Your information is fully available to the issuing bank, the merchant, the credit card network, and law enforcement – if subpoenaed. In this regard, bitcoin is anonymous but not private. Identities are not revealed in the blockchain – but every transaction is visible. A bitcoin user connecting with their personal information to centralized exchanges or using online wallets has now inadvertently given up their right to both privacy and anonymity. As a result, there is little difference in anonymity between using Bitcoin and using a bank to transact.

With this understanding that bitcoin is not anonymous, different methods and techniques have been utilized for those with sufficient motivation to obfuscate their transaction history with the help of mixes or tumblers. A mixer allows users to entrust a set of coins to a pool operated by a central party

and then, after an interval, retrieve different coins with the same total value. Unfortunately, the mixer can still trace coins, and the mixer can also steal coins.

Decentralized vs Centralized

"We will spread ourselves across the Planet so that no one can arrest our thoughts."

-John Perry Barlow - A declaration for the independence of cyberspace[6]

Decentralization is a core principle of cryptocurrency. But what does that mean and why is it important? Modern banking with fiat currency is a centralized system. One entity controls the use and even the destiny of the currency. Even at a more personal or local level, your own bank controls your access and ability to transact with your money. The idea of a decentralized ledger takes away the ability for one entity to control the supply, distribution, or fungibility of the currency that is on the ledger. Decentralization also applies to the development of cryptocurrency, as all the involved parties (or nodes, really) have to have a majority agreement of even what software version is being used.

So, the benefit of decentralization also has some drawbacks. One is that because of the need for a majority of nodes to be in agreement, if there is another group of nodes that don't want to agree with the first, but want to continue their own blockchain ledger, a "chain split" or "fork" occurs. Now there are essentially two versions of a cryptocurrency. These forks have occurred over disagreements about what future development of a coin should look like, so these arguments can slow the development of a project and render it unreliable for significant transactions.

With that said, because decentralization is such an important, even the most important, aspect of cryptocurrency, every effort must be made to make a blockchain that is as advanced and yet as secure as possible early in its development. While there is no such thing as "future-proof," SafeCoin has built on the strengths of others in the open-source cryptocurrency community and added and changed things to be as forward-thinking as possible, with the same open-source doctrine as other cryptocurrencies before.

Why SafeCoin?

SafeNodes: Real-World Blockchain Security

One of the biggest threats to every cryptocurrency (and associated blockchain) is the constant possibility of a double-spend attack. SafeNodes will make double-spend attacks on SafeCoin nearly impossible. Building upon the notarization nodes of Komodo, SafeNodes are a novel solution to a common problem.

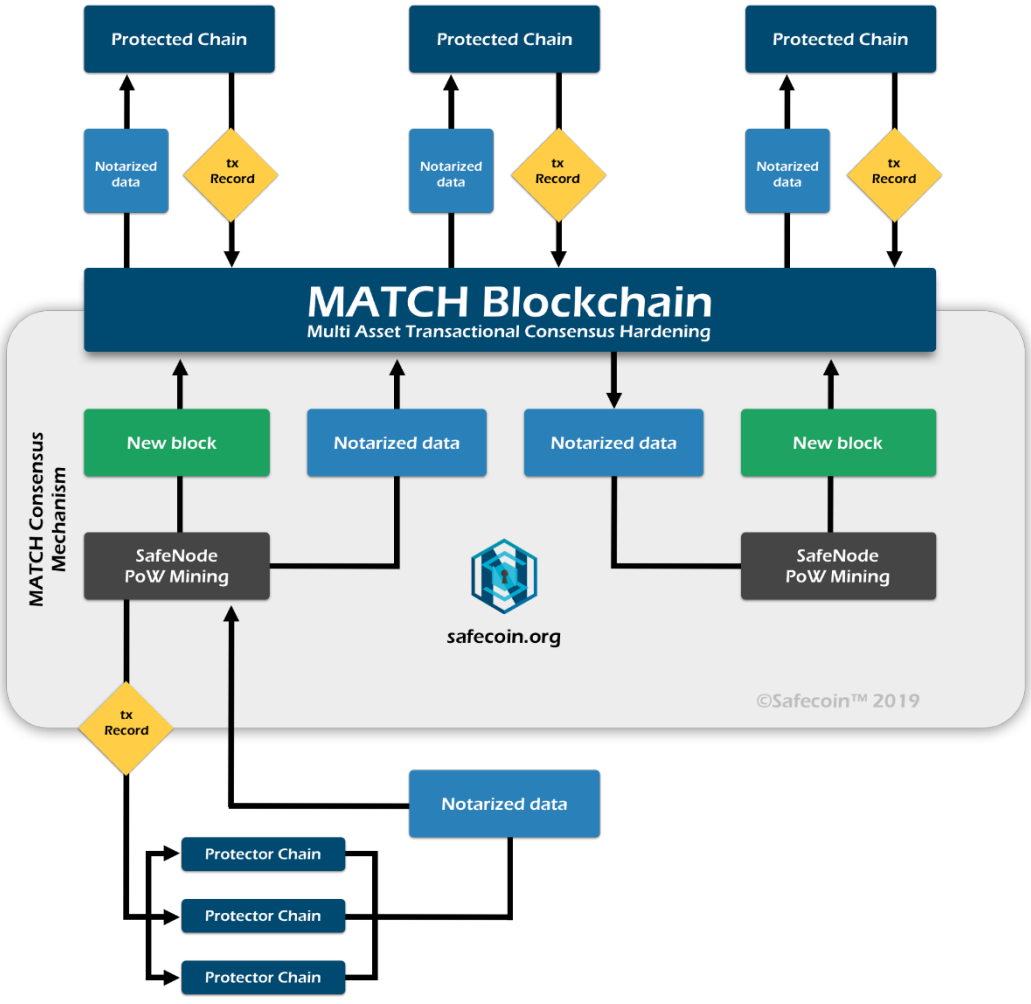
SafeNodes are the world's only cost-free, sustainable, and efficient solution for protecting proof of work blockchains from double-spend attacks. They are designed to be the world's first cross-chain linking solution which notarizes Bitcoin and other blockchains with the goal of making crypto safe. By working together with the same spirit of cooperation that open source is founded on, they can all be protected.

The Multi-Asset Transaction Consensus Hardening (MATCH) protocol leverages a tremendous level of security by combining the hash rate and security of several blockchains into a solid guard against 51%

attacks and related double-spend attempts. The MATCH protocol calls for SafeNodes to take a snapshot of the SafeCoin blockchain, and a hash of that snapshot is then written into a block on other blockchains. This happens in a continuous manner, on several blockchains, but without a set timing interval. The process of notarizing at different times to different blockchains creates multiple fallback points on varying blockchains. A potential attacker would have to take down every single layer of protection at roughly the same time before the SafeCoin blockchain can be successfully attacked. This means the SafeCoin blockchain can benefit from the most secure blockchains in the world at a fraction of the cost. SafeCoin is the first blockchain to use MATCH technology.

Other blockchains can benefit and even profit from this enhanced level of security via a process called Cross-Chain Linking. The process of notarization is multidirectional. Additionally, one blockchain can be the notarizing gateway for other blockchains. This allows Blockchain A to benefit from Blockchain X, Y, and Z´s security level by only notarizing to Blockchain B. Cross-Chain Linking represents a very cost-efficient method to secure blockchains with a high-security standard.

The value of having a blockchain secured by MATCH cannot be overstated. The protection against a double-spend attack allows exchanges to validate deposits with far fewer confirmations and allow businesses to have confidence with a near-instant transaction.



Best Privacy Technology

Safecoin includes the Sapling protocol, the latest protocol available for zk-SNARKS [3]. zk-SNARKS allow for provably private transactions between sender and receiver. SafeCoin continues to develop the integration of TOR and TLS protocols, further protecting privacy. TOR obfuscates a user's IP address, preventing the tracking of IPs relating to a transaction. The TLS protocol is a secure connection between nodes, preventing man-in-the-middle attacks, and encrypting transaction details.

Coin Specifications

Hash Algorithm	Equihash 192_7
Consensus	PoW, MATCH, PoS
Privacy	zK-SNARKS + Jumblr
Nodes	SafeNodes (3 Tiers: 10k, 50k, 100k)
Block Time	60 Seconds
Total Supply	36 Million
Block Reward	4 SafeCoins (as of 2019)

SafeCoin Platform - Protocol

Many cryptocurrencies preceding SafeCoin have pioneered innovations that have yielded network architecture, distributed ledgers and consensus mechanisms for storage, transmission, and security.

SafeCoin has selected the best of these innovations in establishing our technology stack and platform, ensuring we evolve from established development efforts and innovate further in ensuring SafeCoin's

long-term viability. The SafeCoin team thanks and acknowledges the foundational projects: Bitcoin, Dash, Komodo, SuperNET, Horizen (Zencash) and Zcash. Through further community support on these projects, it can ensure that SafeCoin innovations add to the global community pool of knowledge by remaining owned by the public domain, which is a shared Satoshi vision.

Komodo

Komodo Platform, a Zcash clone, has always been a leader in the blockchain space with a long history of delivering one groundbreaking technology after another. While some cryptocurrency projects are only now becoming aware of the blockchain industry's most pressing challenges, like interoperability and scalability, Komodo recognized them years ago and has been working tirelessly to provide solutions ever since

The SafeCoin team recognized these same challenges early on, and after extensive research and careful consideration, decided that the Komodo Platform offered the best choice for building a foundation that would allow SafeCoin to achieve its ultimate vision.

Zcash

Zcash extended Bitcoin with fully anonymous shielded transactions so that users could choose between normal Bitcoin-like addresses (T-addresses) or shielded addresses resistant to traffic correlation analysis (Z-addresses).

T transactions

T transactions are the traditional blockchain-recorded transactions controlled by a private key in a wallet. These are derived from Bitcoin and enable rapid compatibility with exchanges, wallets, and other Bitcoin-derived ecosystem applications.

Z transactions

These are transactions sent to shielded addresses, as inherited from Zcash and Zclassic. Balances in shielded addresses are private. If spending to one or more shielded addresses, the value stays private but any transparent addresses on the receiving end will de-shield the token and reveal the value received on the blockchain. The input shielded addresses and whether the value was sent from one or two of these remain confidential when de-shielded.

The Zcash counterfeiting vulnerability that was discovered in 2018 and remedied by Zcash has been remedied in the SafeCoin code, as well. To ensure the integrity of the SafeCoin blockchain, all funds had to be removed from private addresses and sent to transparent addresses before the private addresses were deactivated. Prior to implementing the updated code, an audit of current coin supply was done, verifying that the exploit had not been taken advantage of before the updated private addresses were available.

SafeCoin can utilize all this technology as it strives to be the standard in safety and while providing enhancements, innovations, and leveraging a passionate and talented community.

No other coins have ever distributed this much-advanced technology fairly for adoption by the community without ICOs or hidden fees.

- SafeCoin only established a small transparent and published pre-mine (4 million Safe) for bounties, airdrops, marketing, exchange listings, enhancements, and innovations.
- No ICO
- No sales of any kind
- Fair distribution
- No mining tax or treasury
- No derivative fees
- A fixed cap of 36m supply

SafeCoin builds upon these already tested protocols and adds in the SafeNodes using MATCH protocol, TLS encrypted wallet communications, privacy, mixing, and multiple user wallets.

SafeTrade

SafeTrade is a new cryptocurrency exchange developed by the SafeCoin team. SafeCoin is the main trading pair of the SafeTrade exchange. Our team is committed to utilizing the highest levels of account security to set the standard for service, reliability, and customer-centric driven updates. High deposit confirmations, low automatic withdrawal amounts, and two-factor authentication are the standard ways of keeping exchanges and users secure, but at the cost of convenience. As crypto projects become more secure using notarization techniques, SafeTrade will be able to make a user's experience more convenient yet still safe. We will eventually be fully reporting to all appropriate government agencies with an eye towards complete compliance with all local laws.

SafeCoin Wallets

The primary wallet that many people will use is known as a "full node" wallet, and it contains everything that SafeCoin needs to send and receive SafeCoin, including a current synchronized copy of the blockchain, which enhances network strength, availability, redundancy and speed. The SafeCoin desktop wallet includes several additions and refinements. An example of these refinements is the ability to run a SafeNode in a simple and convenient way.

Finally, SafeCoin has developed a multi-coin wallet based on the open-source Bitpay Copay wallet. The SafeCoin implementation can already be used with over ten cryptocurrency coins. This wallet works in a web browser, as an Android app, and as an iOS app. This wallet is one of the most comprehensive and easy to use wallets available. The SafeCoin team has a goal of this wallet, including every coin that is available on SafeTrade.

SafeCoin Community P2P / B2B

"We believe that from ethics, enlightened self-interest, and the commonwealth, our governance will emerge."

-John Perry Barlow - A declaration for the independence of cyberspace[6]

SafeCoin's most powerful resource is a fantastic and talented growing community of individuals who care about our future and privacy rights, and are working hard to make this world a better place through their contributions at SafeCoin. As a fully open and inclusive project, all kinds of contributions and support have flowed into our community from around the world.

We are growing by the minute, attracting talented developers, miners, traders, long-horizon investors, partner organizations, exchanges, bloggers, etc. Our community already has an enduring history not only of positive relationships and friendly interactions but also of spontaneous support and engagement emerging to prevent or solve disparate problems.

Future Development of SafeCoin

Forecasting is a challenging exercise, but we see a bright future for SafeCoin and the thriving and secure ecosystem we're building. We believe that the decentralized, fully inclusive, voluntary, and flexible organization we're creating will be the standard in the near future.

The advent of blockchain technology makes such a thing possible, and we believe many people already do and will share our vision for a better world, especially when they see how we can accelerate innovation and improve human welfare by empowering everyone with privacy, anonymity, and freedom to express their values.

We are dedicated to executing our Roadmap and doing everything in our power to see this vision come to fruition. There are sure to be challenges along the way. There already have been. However, flexibility, passion for our values, and peaceful cooperation will consistently carry us through adversity. We are fortunate to live in an age of incredible innovation in both technology and ideas.

Upcoming:

- SafeNodes- full implementation
- Revised Roadmap for 2020 and beyond
- Technical whitepaper on SafeNodes and the MATCH protocol
- Integrations with SafePay
- Tor Network Anonymous Communication
- Enhanced end-to-end Tor integration for improved private connections and traffic
- OBFS4 Integration
- SafeTrade 2.0
- Merging technology to expand exchange into mainstream markets
- Swiftcoin development and implementation for ultra-fast, private transactions
- Decentralized Trust protocol
- FairExchange - A decentralized exchange that will be integrated with SafeTrade
- Expand SafeCoin into charitable causes
- New Safecoin.org website

  *this is an ever expanding list as we examine and improve solutions

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

[2] https://komodoplatform.com/wp-content/uploads/2018/05/2018-05-09-Komodo-White-Paper-Full.pdf

[3] https://whitepaperdatabase.com/zcash-zec-whitepaper/

[4] https://explorer.safecoin.org/block/09f5deffb9c816d82b8f696befa84681509274288c4529f213aeeac57999e8c9

[5] https://github.com/Fair-Exchange/safecoin

[6] J.P. Barlow, “A Declaration of the Independence of Cyberspace”
https://nakamotoinstitute.org/literature/cyberspace-independence/
https://www.eff.org/cyberspace-independence

[7] https://komodoplatform.com/security-delayed-proof-of-work-dpow/

[8] https://cacm.acm.org/magazines/2018/7/229033-majority-is-not-enough/abstract