SafeNode Technical Whitepaper

May 4th 2018

Alpha Version: 0.21

Note: All technical aspects in this document define main features of the SafeNode project and will also specify the reward distribution system.
*This alpha whitepaper will be updated in the first phase of the Safe**Node** project.*

Abstract

The current state of MasterNode networks and projects in more than questionable, when 85% of new launching projects turn out to be a failure. In addition, proof of work based cryptocurrencies offer more risk on attacks against their blockchains due to high computational power owned by big companies or conglomerates with large amounts of hashpower or ASIC mining farms. In these days more than a few individuals are able to put the network at risk, to the cost of all. In this paper, SafeNode aims to propose a solution to these issues.

1. SafeNode Introduction

Safe**Node** is a truly anonymous digital currency focused on 100% private and untraceable transactions. Based on a POW/POS hybrid system, first implemented on PIVX, Safe**Node** utilizes its own *Safe**Nodes** to* ensure the network stays decentralized and is secured against attacks of all kinds. Alongside the staking based algorithm for its primary long-term use case we focused on creating a secure network governed by the community for future updates on the core development.

That's why we developed *Safe**Node***.

a) **storage** of **value** – safe and secure through cryptographic encryption, where nobody besides the owner of the private keys can control any of the stored assets. (4a)

b) **bigger picture** – every year bitcoin and crypto-mining burns up more than 140 terawatt-hours of energy, which is 0.6% of the worlds entire power use and almost as much as all Baltic States together needed in 2016. Our Proof-of-Stake (POS) reward mechanism allows holder of **XSN** to contribute hashpower to the Safe**Node** chain through validating transactions according to the amount of **XSN** locked inside the Safe**Node** Wallet. (4b)

c) **stay private** – most blockchain transactions are anonymous, yet they are not private, but why? Compared to regular financial systems a blockchain works without identities behind transactions, though everybody can look into transactions on the blockchain. If just one transaction can be linked to a real life entity, it is possible to trace back the real identity behind those transactions. The Zerocoin protocol prevents this scenario by creating new coins from old ones – unable to trace back at all cost. (4c)

2. Comparing POW to POS

The proof of work system used in most cryptocurrencies, is a mining and computer power-based system in which miners are required to solve difficult mathematical problems to validate and authenticate transactions on the blockchain. It was integrated because it provides complete decentralization of power and control over the distribution and implementation of major technical and economic changes in the network. If an attacker wants to hack a cryptocurrency network today, for instance, the bitcoin network, he would have to gain 51% of the computing power. This can be made possible if some of the largest mining pools join together to attack the network. While this is highly unlikely politically, technically, it is still a possibility.

If the Proof-of-Work is based on mining and computing power, the Proof-of-Stake derives from actual holdings of the cryptocurrency. That means users that own the largest chunk of coins in the network would have the authority to make network changes and mine an equivalent portion of their funds regardless of computing power. For example: user who own 20% of all XSN would be able to mine 20% of the Safe**Node** network's transactions gaining 1/5 of the network power and has also a significant impact on the implementation of economic and technical changes within it. In a Proof-of-Work network, the majority of voting power when implementing important changes to the system is divided among miners, developers and other crucial members of the community. Proof-of-Stake eliminates some of the major security issues associated with the Proof-of-Work, most important is the 51% attack.

2. Coin Specifications

Name	Safe**Node**
Symbol	SXN
Algorithm	x16r
Block Time	60 Seconds
Block Maturity	60 Blocks
Difficulty Retargeting	Every Block
Premine	210,000 SXN (1%)
Maximum Emission (POW)	200,000 SXN (premine excluded)
Maximum Emission (POS)	20,590,000 SXN
SafeNode Reward	60 %
SafeNode Collateral	10,000 SXN

3. Reward Distribution

Blocks	Amount
0	210,000 SXN
1 – 500	2 SXN
501 – 10,000	20 SXN
10,001 – 650,000	15 SXN
650,001 – 1,300,000	10 SXN
1,300,001 – max. reached	5 SXN

4. Technology

a) Safe**Nodes**

Safe**Nodes** are the base of our blockchain network acting as a manager for the system while also performing special jobs and earning SXN as a reward for Safe**Node** holders.

Safe**Nodes main tasks*:**

- Managing Role on proposals to improve Safe**Node** blockchain - ***Governance***
- Special Jobs
    - Instant Transactions - ***InstantSend***
    - Private Transactions - ***PrivateSend***

b) Proof of Stake 3.0

Proof-of-Stake eliminates the need for miners on the network to validate transactions. The first cryptocurrency to implement the POS method was Peercoin, after which other forks have been adapted upon. Right now Blackcoin's Proof-of-Stake 3.0 have solved the issues faced with Coin-Age, Block Reward and Blockchain Precomputation. The protocol is robust and keeps nodes connected to the network. The entire purpose of a secure and fair financial system is to place control of it in the hands of the people now with the incentive to stay connected, shareholders get greater benefits across the board.

c) ZeroCoin Protocol

ZeroCoin started as a project to fix a major weakness in Bitcoin: the lack of privacy. Something we take for granted in using real cash. A collaboration between the the original ZeroCoin project members and cryptographers at MIT, The Technion, and Tel Aviv University, has produced a far more efficient protocol that allows for direct private payments of hidden value between parties. ZeroCoin allows for coin-mixing with zero knowledge transactions to be made on SafeNode. Each user can convert (non-anonymous) XSN into (anonymous) coins. Users can then send „ZeroCoins" to other users, and split or merge ZeroCoins they own in any way that preserves the total value. This means that every SXN transaction using ZeroCoin is 100% private and has no prior transaction history attached to it.

5. Milestones

Near Future

- globally distributed secure network
- involving community members in further development
- strong marketing campaign with experts and testimonials
- activate ZeroCoin protocol and start governance platform for voting
- release new projects to vote with and for SafeNodes

Future

- real life implementation through mobile wallets
- smart contracts activation on payment gateways
- *To guarantee full on implementation of our features we need to activate at least 1000 SafeNodes on the SafeNode blockchain over the course of the first two years.

Conclusion

SafeNode aims to provide a safe and secure blockchain environment bringing cryptocurrency to a larger audience while maintaining a consistent value to owners and stakers. With multiple use cases ahead, the first and most important step is to build a strong community to become and sustain a big player amongst cryptocurrencies. By implementing real world applications for real world problems we will not only provide modern features but also develop further more improvements on our Safe**No**de system.

References:

http://zerocoin.org/
https://peercoin.net/assets/paper/peercoin-paper.pdf
https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf
https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf