SchillingCoin – The environment friendlier Cryptocurrency with Proof of Stake

May 1st, 2018

Abstract

A environment-friendlier approach at peer-to-peer cryptocurrencies derived from Satoshi Nakamoto's "Bitcoin". Proof-of-stake replaces the widely, energy hungry, standard of "proof-of-work" to provide security to the network. Under our hybrid design proof of work is being only used for the "minting" of coins. The security level of the network is not depending on the amount of energy that is consumed in the long run, therefor it provides a energy-efficient alternative to common cryptocurrencies. Proof-of-stake is based on the coins age and is being generated by each node via a hashing mechanism which bears similarity to Bitcoin's one, but over a limited search space. The blockchain history and transaction settlement are further protected by a centrally broadcasted checkpoint mechanism.

Introduction

For almost 10 years, since the creation of the first widely accepted cryptocurrency – Bitcoin -, proof of work has been the most predominant design of cryptocurrencies. The concept of proof-of-work has been the backbone to minting and security model of Nakamoto's design.

Just a few months after Nakamoto released his design of bitcoin, the team of Peercoin – the project we forked from – realized that the concept of coin age can facilitate an alternative design known as proof-of-stake, to Bitcoin's proof-of-work design. Since then a system has been formalized where proof-of-stake is used to build the security model of a p2p cryptocurrency and part of its minting process, whereas proof-of-work mainly facilitates the initial part of the minting process and gradually reduces its significance in the network.

This groundbreaking design attempts to demonstrate that viability of future and upcoming peer-to-peer cryptocurrencies with no dependency on high energy consumption. This project has been named "SchillingCoin".

Coin Age

The amount of the totally hold coins times holding period equals the so-called "coin age". This concept has been known from at least as early as 2010 to Nakamoto and has been used in Bitcoin for example to help prioritize transactions, although it did not play a critical role in Bitcoin's security model.

Example:

If Bob receives 100 Coins from Alice and holds it for 90 days, Bob has accumulated 9000 coin-days of coin age. When Bob spends the 100 coins, the accumulated coin-age is being consumed (or destroyed).

In order to facilitate the computation of coin age, a timestamp field has been introduced into each transaction. Block timestamp and transaction timestamp related protocols are strengthened to secure the computation of the coin age.

Proof-of-Stake

Nakamoto's major breakthrough was the use of proof-of-work, which unfortunately leads to a energy-dependent cryptocurrency and thus adds a significant cost overhead in the operation of such networks. As the mint rate slows in the Bitcoin network, eventually it can put pressure on raising the transaction fees exorbitantly to be able to sustain a preferred level of security.

The whole approach of proof-of-work on peer-to-peer cryptocurrencies is not mandatory and with proof-of-stake we would like to demonstrate that it is an important milestone both theoretically and technologically to the future of cryptocurrencies.

The proof-of-stake termed concept has been discussed among Bitcoin circles as early as 2011. Roughly speaking the term proof-of-stake means a form of proof of ownership of the owned currency. The coin age which is consumed by a transaction can be also considered a form of proof-of-stake. The concept of proof-of-stake has been independently discovered around October 2011, whereby most of the Bitcoins minting and security model has been replaced by redesigned proof-of-work functions. This is mainly because similar to proof-of-work, proof-of-stake cannot be easily forged. This is one of the main critical requirements of monetary systems - being difficult to counterfeit.

Proof of Stake - Block generation
In this hybrid design, blocks are separated into two different types, proof-of-work blocks and proof-of-stake blocks.

A new type of special transaction called "coinstake" has been added to the proof-of-stake typed blocks. In the coinstake transaction block, the owner pays himself thereby consuming his coin age, while gaining the privilege of generation a new block for the network and therefor minting for proof-of-stake. In the coinstake block, the first input is called "kernel" and is required to meet certain specified hash targets in the protocol, thus making having the block generation being a stochastic process, which in the end is similar to the block generation of proof-of-work blocks.
However an important difference lays in the hashing operation being used, which is processed over a limited search space (1 hash per unspent wallet-output / second), instead of an unlimited search space as default in proof-of-work protocols. Therefor, there is no significant energy consumption involved.

The required hash target, that the stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (opposite from Bitcoin's proof-of-work, which is a fixed target value applying to every node). By using this design we ensure that the more coin age is consumed in the kernel, the easier it is to meet the hash target protocol.
Example: Bob has a wallet-output which accumulated 100 coin-years and expects it to generate a kernel in 2 days, then Alice can except her 200 coin-year wallet-output to generate a kernel in a single day.

Contrary to bitcoin's proof-of-work which adjusts its hash target on a fixed schedule of 2 weeks, we designed Schillingcoin's adjustment to be continuously, thus avoiding any sudden jumps in the network generation rate.

Proof-of-Stake Minting

In SchillingCoin we introduced a new minting process for proof-of-stake blocks in addition to Bitcoin's used proof-of-work minting. PoS blocks mints coins based on the consumed coin age in the coinstake transaction. A mint rate of 1% per consumed coin-year is chosen to give rise to a low future inflation rate.

Even tough we kept proof-of-work minting as a part of the minting process, it is conceivable that in a pure proof-of-stake system, the initial minting can be seeded completely in genesis block via a process similar to stock market initial public offers. (IPO)

By applying this design feature, we alleviate some of the concerns regarding Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of the networks hashing power.

First of all, the cost of controlling a significant stake might be higher than the cost of acquiring significant hashing power, thus raising the cost of an attack for such powerful entities. The coins age is also considered during the attack, which may render it more difficult for a potential attacker to continue preventing transactions from entering the main blockchain.

Protection of transaction History: Checkpoints

The biggest disadvantage of using total consumed coin age to determine the main blockchain is that it lowers the cost of an potential attack on the entire chain of history. Even though Bitcoin has a relatively strong protection over the history, its creator - Nakamoto - still introduced so-called "Checkpoints" in 2010 as a additional mechanism to solidify the blockchain history, to prevent any possible changes to the part of blockchain earlier than the checkpoint.
Another concern is that the cost of double-spending attacks may have been lowered as well, as a potential attacker may just need to accumulate a certain amount of coin age, and thus forcing reorganization of the blockchain. To make commerce practical under such systems, we decided to introduce an additional form of checkpoints that are broadcasted by a central authority, at much shorter specified intervals such as a few times daily, to be able to freeze the blockchain and finalize transactions. This new type of applied checkpoints is broadcasted similarly to Bitcoins 'alert' system.
For SchillingCoin we attempted to design a practical distributed checkpointing protocol, but found it difficult to secure against network split attacks. Although our broadcasted checkpointing mechanism is a form of centralization, at the time of writing this paper, we consider it an acceptable solution before a distributed mechanism is available.

The use of centrally broadcasted checkpointing’s has some other technical reasons. To be able e to defend against different types of denial-of-service attacks, the coinstake kernel must be verified before a proof-of-stake block can be accepted into the block tree of each node. Due to Bitcoins node data model (transaction index specifically), a deadline of checkpointing must exist, to ensure all nodes capability of verifying connection of each coinstake kernel before accepting a new block into the block tree. Because of the above considerations, we have decided to let the node's data model untouched and not modify it, but instead to use central checkpointing. Our solution to this design is to modify the coin age computation to require a minimum age, such as one month. Then the central checkpointing is used to ensure that all networks nodes can agree upon past transactions older than one month, thus allowing the verification of coinstake kernel connections, since a kernel requires non-zero coin age, thus it must use an output from more than one month ago.

Duplicate Stake Protocol and Block Signatures

Every block has to be signed by its owner to prevent the same proof-of-stake block from being copied and thus used by a potential attacker.
A duplicate-stake protocol is designed to be able to defend against a potential attacker using a single proof-of-stake to generate multiple blocks as a denial-of-service attack. Each connected node collects the pair of all coinstake transactions it has seen. If a received block contains a duplicate pair as another previously received block, it ignores such

duplicate-stake block until a successor block is received as an orphan block.

Energy Efficiency

As soon as the proof-of-work mint rate approaches zero, there will be less and less incentive to mint proof-of-work blocks. By taking this long-term scenario in consideration, the energy consumption in the network may drop to very low levels as miners stop mining proof-of-work blocks out of disinterest or financial reasons. The Bitcoin network faces such risk, unless transaction volume or the fees rise to high enough level to sustain the energy consumption. The SchillingCoin's design ensures that even when energy consumption reaches zero, the network is still being secured by proof-of-stake. A cryptocurrency is long-term energy-efficient if energy consumption on proof-of-work blocks is allowed to approach zero.

Other Considerations

The proof-of-work mint rate has been modified to be not determined by the current block height (time), but instead by difficulty. When mining difficulty goes up, the proof-of-work mint rate is lowered. A smooth curve is chosen in contrast to Bitcoin's step functions, to avoid artificial market jumps. More specifically, a continuous curve is chosen, such that each 16 times raise of mining difficulty halves the block mint reward. Over long-term, the proof-of-work mint curve will not be too dissimilar to that of Bitcoin in terms of its inflationary behavior, given the continuation of Moore's Law.

Some studies revealed that transaction fees are an incentive for the cooperation of miners. Under SchillingCoin's system we have removed the reward of transaction fees to the block owner, to remove possible attacks. Therefor we decided to destroy the used transaction fees instead. This removes the incentive to not acknowledge other minter's blocks, and it also serves as a additional deflationary force to counter the inflationary force from the proof-of-stake minting. The transaction fees are also enforced at protocol level to be able to defend against block bloating attacks.

Conclusion

Upon validation of our unique design in the market, we expect proof-of-stake design to become a potentially more competitive form of peer-to-peer cryptocurrencies, due to the elimination of dependency on energy consumption, thereby achieving lower inflation/lower transaction fees at comparable network security levels.

References

Sunny King, Scott Nadal (2012): PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake
https://peercoin.net/assets/paper/peercoin-paper.pdf
Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)