Proof-of-Stake Protocol v3.0

Abstract

Proof of Stake's security has proven itself reliable & effective over years of testing while at the same time solving Bitcoin's issues caused by the Proof of Work (PoW) protocol. The latest Proof of Stake (PoS 3.0) advances pioneered by Blackcoin that are now integrated into Bitbay have solved the issues faced with Coin-Age, Block Reward, Blockchain Precomputation. The PoS 3.0 protocol is now robust and keeps nodes connected to the network while disincentivizing inactive nodes. In this paper we will highlight the mechanisms & advantages of PoS 3.0.

I. Introduction

Cryptocurrencies have managed to change the way finance and money is defined. The advent of Bitcoin [1] has showed how a peer-to-peer network can prevent forgery by solving the "Byzantine Generals Problem." Since then many different coins have been created based on Bitcoin's open source code.

There are two major methods to secure the blockchain network.The first is "Proof of Work" and the second is "Proof of Stake". The theory behind PoW is to hold a mathematical competition. The first computer to solve the puzzle is the one that confirms the block of transactions and wins the coin reward of it. This is called mining. However, this creates a problems of wasted high resource cost, wasted high energy cost, high fees, slowness (slow processing of transactions, slow tx/sec) and ends up centralizing the network into a few pools of computers owned by a few rich persons that could afford all the hardware bills, all because of the very nature of mining.

On the other hand, PoS 3.0 is a competition between coinholders, where based on connectivity to the network and random chance, you can confirm a block of transactions and receive coin rewards. This is called staking. It doesn't necessitate any particular hardware except a normal computer with an internet connect and you are guaranteed to be rewarded proportionally the amount of coins you hold which makes it fair and decentralized. Coin rewards are determined by a yearly supply inflation and awarded proportionally to addresses that stake (equivalent of mining in PoS 3.0).

For example, Bitbay yearly staking rewards is set to 1% of the supply, so in the scenario where everyone stakes you would receive yearly 1% of your coins as reward, although not everyone stake so it is in average more than that because if not everyone stakes, then you propertionaly receive additional coin rewards (if only 20% of the network stakes with a 1% stake rate, then you would receive 5% of your coins as reward if you stake). In addition to that, stakers (those who stake) are rewarded the transaction fees of the network.

PoS 3.0 solves PoW problems of Bitcoin as it manages to be fast and low cost while remaining decentralized. We will now proceed to highlight the great security of PoS 3.0 and how it solves the related security problems.

II. Security, coinage and attacks

The whole purpose of holding competitions for coins is to avoid attacks. Confirmation of transactions is an honor given to the winner of a block. Although if this system can be gamed, then it is flawed.

In PoS, you first prove you have access to coins and from that point you can compete to win blocks randomly. The more people competing the more secure the block. Coin age is the idea that the longer you hold coins the higher the probability you can win a block. Its original intention was to incentive dormant holders of coins. However, this does not encourage a node to stay connected to the network in practice since they can wait for the reward to increase. Also, coinholders can disconnect from the network for long periods of time, then reconnect and win enough blocks to risk a 50% attack on the network. The time calculation will effect payouts discouraging connectivity. Also, the fewer the nodes that are connected, the easier it is to gain a majority of the blocks forging consensus. Also, stakes can be computed in advance to make the attack more effective. Timestamps are used in PoS to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps.

In PoW, a difficulty increase or decrease is made depending on how quickly a block was produced. However, as a precautionary method to prevent any sort of "Timing Attacks" PoS development teams use centralized checkpoints.

III. All problems have a solution

A. Coin Age

Coin Age is calculated by the weight of unspent coin and the time they have been dormant. The calculation is simply "proofhash < coins · age · target".

The proof hash is the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. The attack of saving up Coin Age was previously outlined as improbable [2]. The reasoning behind this is because it is very difficult to perform consecutive double spending since Coin-Age would reset after the first expense. Although this is not entirely clear because an input can be split into 1000s of outputs. This may give the possibility for consecutive double spend attacks. However, this is still a difficult problem because the attacker would need a significant amount of funds to hold weight greater than the network. In theory, this makes sense. Although If we look at the amount of forks using PoS, we can see the amount of nodes are fairly low and this gives much greater weight to a smaller handful of nodes. A holder of many coins may not want to perform this attack since they run the potential of losing value of their coins if detected. However rational this may seem, it is probably a fallacy because it is still an attack vector and a very real one indeed. More importantly, with so many coins being published daily, keeping as many nodes connected as possible is imperative to security.

Solution from PoS 2.0: Removing Coinage from the equation - "proofhash < coins · target".

B. Blockchain Precomputation

The block timestamp is key to the PoS system. It is possible in theory to fork a coin by changing previous timestamps. The stake modifier does not obfuscate the hash of sufficiently to prevent knowing future proofs. So an attacker can attempt to compute all of the blocks in advance and run a higher probability to forge multiple consecutive blocks. Solution from PoS 2.0: The stake modifier is changed at every modifier interval to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake. The expected block time was increased from original 60 seconds to match the granularity.

Past limit: Time of last block
Future limit: +15 seconds
Granularity: 16 seconds (effectively increased from 1 second)
Expected block time: 64 seconds

C. Block Reward

The Block Reward in most PoS systems is unfortunately based on Coin Age. In theory, this is to distribute interest fairly by allowing nodes to receive latent payments due. It is an attempt to keep a common APR. However, this system does not work because nodes can stay disconnected and with many split inputs, reconnect to the network and game the reward system. Also, it does not give nodes any incentive to stay connected. In a decentralized system, the more nodes connected the better the security since it shifts trust from a single entity to the network itself. Solution from PoS 3.0: The block reward was made a constant 20 coins per block. This was based proportional to the supply of coins maintaining interest at %1.

IV. Multisignature & Cold Staking

The final noteworthy addition to the protocol was the implementation of "Multisignature Staking".

One drawback to many staking algorithms is they only support staking with a single key. Since the popularity and use of Bitbay [3] which uses a two party escrow system also known as "Double Deposit Escrow" and extremely secure dual key accounts, it has become important to allow these accounts to participate in securing the network. Beyond dual key accounts there are many other types of inputs that make use of p2sh and lock times and those must also be allowed to secure the network as well. The other problem is that in a single key account, a hacker can use key-loggers to obtain your password and compromise your wallet while it is unlocked for staking.

Solution from PoS 3.0: We allow users to place the block signing key in the output of "6a" known as a burn address so they can stake by sending a standard transaction.

This allows any input to be eligible for submission. This gives Bitbay a huge advantage for custom staking software, voting and the legendary "Cold Staking". The "Cold Staking" technique involves multiple computers. Basically when a multisignature input is eligible for staking, the signatures are split up between many computers. This makes an account virtually impossible to hack because even if a single key was compromised, the other keys are in a completely different location either on the local area network or on multiple servers. This technology is already implemented in Bitbay.

V. CONCLUSION

The elimination of Block Reward based on time was an obvious improvement. Therefore, if the amount of nodes staking drops, yearly interests to active nodes would increase proportionally. For example, if only 1/5th the network was staking, you can expect up to 5 times the reward! In contrary to the many PoS coins that do not have enough nodes, this PoS 3.0 feature is a great advantage to small coinholders. Although the lack of statistical data conserning PoS coins, it is self-evident that there is usually less than 20% of the coinholders staking. In PoS 3.0 the aformentionned increase in incentive will keep the nodes more numerous, more competitive and hence more decentralized. The change in granularity was useful to prevent "Stake Grinding". Even with all the hashing power of the Bitcoin network, using PoS 3.0 a network attack in practice would be extremely unlikely to the point of being realistically not possible.

PoS 3.0 is one of the most secure and reliable system ever created and Bitbay greatly benefits from it. Everything is done to ensure anonymity, to keep as many nodes connected as possible, to guarantee decentralization and to mitigate all attacks. Decentralization was the original core ideology in Bitcoin, but sadly, Bitcoin’s flaws prevented it to prevail in the long run. The entire purpose of a secure and fair financial system is to place control of it in the hands of the people so that it be for the people and by the people. Thankfully PoS 3.0 has solved the main issues of Bitcoin’s PoW while ensuring its own future by providing an incentive to stay connected to the network in order to keep it secure and decentralized.

References:

[1] Satoshi Nakamoto ~~~ Bitcoin: A peer-to-peer electronic cash system. bitcoin.org, 2008
[2] Pavel Vasin ~~~ Proof of Stake 3.0: http://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf, 2013
[3] Bitbay.market