Security Analysis of Proof-of-Stake Protocol v3.0

Impleum
https://impleum.com/
08/12/2018

Abstract

Proof of Stake's security has proven itself over years of testing. Advances in this technology in Impleum'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. It disincentives inactive nodes. In this paper we will highlight and outline the advantages and perform a security analysis of the system. We also outline ideas here in **Impleum** to potentially increase security further.

I. Introduction

Cryptography has managed to change the way finance and money is defined. Recently 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 for generating new funds on the network. The first is "Proof of Work" and the second being "Proof of Stake". The theory behind Proof of Work is to hold a mathematical competition. The first computer to solve the puzzle receives the coins. This makes distribution of coins a completely fair process. However, this also creates a problem of wasted energy. Computers in order to compete, create and arms race of hardware. Thus, money and energy is wasted to generate new coins. Proof of Stake is a competition between shareholders, where based on connectivity to the network and random chance, you can receive new coins. Interest is generated based on how much you hold. This solves the energy waste problem in Bitcoin and introduces new challenges in network security. Here at Impleum, we would like to write a technical analysis of the advantages in this protocol and to honor our predecessors, discuss potential improvements and pitfalls. Proof of Stake was first implemented in "Peercoin"[2]. Later, major breakthroughs in Proof of Stake were made in Impleum namely, "Proof of Stake 2.0"[3] and "Proof of Stake 3.0". We have implemented the Proof of Stake 3.0 system because we believe it to be the worlds most secure and efficient method of coin generation. We will outline and highlight the great security of this system and the technical problem it solved.

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. However, if this system can be gamed, then it is flawed. In Proof of Stake, 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. It's 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, shareholders 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 Proof of Stake to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps. In Proof of Work, 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" Proof of Stake coins 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 Coinage was previously outlined as improbable[3]. The reasoning behind this is because it is very difficult to perform consecutive double spending since Coin-Age would reset after the first expense. However, 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. However, if we look at the amount of forks of Impleum and other popular POS systems, 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 share 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 Proof of Stake 2.0:** Remove Coinage from the equation - "proofhash < coins · target".

B. Blockchain Precomputation

The block timestamp is key to the Proof of Stake 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 Proof of Stake 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 Proof of Stake 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 Proof of Stake 3.0:** The block reward was made a constant 5 coins per block. This was based proportional to the supply of coins maintaining interest.

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 software such as BlackHalo[4], which uses a two party escrow system also known as "Double deposit escrow" and more secure dual key accounts, it has become important to allow these accounts to participate in securing the network. Beyond dual key accounts there is 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 Proof of Stake 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 Impleum 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 being implemented in the latest release of BlackHalo.

V. SECURITY ANALYSIS

The elimination of Block Reward based on time was an obvious improvement. Thus, if the amount of nodes staking drops, yearly interest would increase proportional to the disconnected nodes. For example, if only 1/5th the network was Staking, you can expect up to 5 times the reward! Since many coins do not have enough nodes, this is a great advantage even to smaller shareholders. Although statistical data on all relevant coins would be time consuming to obtain, it is self-evident that there is usually a lot less than 20% of the shareholders staking. We think this increase in incentive will certainly keep the nodes more competitive. The change in granularity was useful to prevent "Stake Grinding". A good analysis of the probability of this attack was done in Neucoin[5]. Their claim is that even with all the hashing power of the Bitcoin network, the attack would not be possible. However, a rollback of a few minutes could cause new users to the network unsure of which chain to join. Therefore, Proof of Stake systems use "Checkpointing" which is basically centralized control of the main developer to choose chains that attempt to do this. Of course, this is not an ideal solution. There was a good proposal made in Ethereum[6] for this. They proposed that a new node to the network asks other nodes "off-band" if they are indeed on the correct chain. Using our decentralized markets, it is possible we can get nodes to share this information periodically. The solution will require further investigation. The additional removal of Coin age in general is a secure decision. It is possible to perform a hybrid system of checking popular time servers as well to help calculate drift and require nodes to keep closely synchronized with a general consensus of time. Addition of other random factors based on the blockchain itself may also be a consideration.

VI. CONCLUSION

One of the most secure Proof of Stake systems in the world is being used here at Impleum. We also have several candidate solutions and ideas for improving security further. Here at Impleum, we take your security seriously. We have done everything possible to maintain anonymity, keep as many nodes connected as possible, guarantee decentralization and mitigate all attacks. Decentralization was the original core ideology in Bitcoin, although we feel this ideology has not been completely maintained. The entire purpose of a secure and fair financial system is to place control of it in the hands of the people. Proof of Stake 3.0 has the economic advantage over Bitcoin because it does not waste electricity to generate new blocks, nor does it create unfair competition for new coins. And now with the incentive to stay connected, shareholders get greater benefits across the board.

REFERENCES

[1] Satoshi Nakamoto ~~~ Bitcoin: A peer-to-peer electronic cash system. bitcoin.org, 2008

[2] Sunny King, Scott Nadal ~~~ PeerCoin: https://peercoin.net/assets/paper/peercoin- paper.pdf, 2012

[3] Pavel Vasin ~~~ Proof of Stake 3.0: http://bravenewcoin.com/assets/Whitepapers/ blackcoin-pos-protocol-v2-whitepaper.pdf, 2013

[4] https://www.blackhalo.info/

[5] Kourosh Davarpanah, Dan Kaufman, Ophelie Pubellier ~~~ NeuCoin: the First Secure, Cost-efficient and Decentralized Cryptocurrency: http://www.neucoin.org/en/ whitepaper/download, 2015

[6] https://www.ethereum.org/