Okcash's Proof-of-Stake Protocol w/ LTSS

based on Pavel Vasin POSv2

***Abstract*—The current Proof of Stake protocol has several potential security issues: coin age can be abused by malicious nodes to gain significant network weight to perform a successful double spend. Additionally, due to coin age, honest nodes can abuse the system by staking only on a periodical basis. This does not secure the network. Lastly: in the current system all components of a stake of proof are predictable enough to allow pre-computation of future proof-of-stakes. In this paper a system is proposed to solve said issues.**

I. Introduction

Currently in the crypto currency community it is common understanding that Proof-of-Stake has yet to prove its security, economic value , and overall energy efficiency over time . In the future we will continue to expand and reinforce the new system to ensure that attack vectors get closed before they can be abused maliciously.

This paper is organized as follows. Section II explains the benefits of the Proof-of-Stake concept. In Section III we describe the flaws of the POSv1 implementation which are then addressed in Section IV. Finally we give a summary in Section V.

II. Proof-of-Stake

Consensus in a decentralized digital currency like Bitcoin [1] is achieved by requiring generated blocks to contain a proof that the node which generated the block solved a computational hard task. Unfortunately the concept of the Proof-of-Work (PoW) based system tends to lean towards eventual self-destruction [2].

Proof-of-stake (PoS) aims to replace the way of achieving consensus in a distributed system; instead of solving the Proof-of-Work, the node which generates a block has to provide a proof that it has access to a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called *target*) is specified by the network through a difficulty adjustment process similar to PoW that ensures an approximate, constant block time.

As in PoW, the block generation process will be rewarded through transaction fees and a supply model specified by the underlying protocol ; which can also be seen as interest rate by common definition . The initial distribution of the currency is usually obtained through a period of PoW mining.

A. Related work

The first PoS based currency was PeerCoin [3] which is still in a period of PoW mining. Further development of the PeerCoin PoS protocol lead to NovaCoin [4] which uses a hybrid PoS/PoW system. BlackCoin was the first crypto currency that used a pure POS based protocol enhancing the POS system further.

Okcash is based on the development of the above described projects while adding a Long Term Staking System (LTSS) [6] to further improve the stabilization and sustainability of the network/chain.

III. Security Issues in PoS

Besides the clear advantage of PoS over PoW as a method used to establish consensus on the network, there exist problems that have yet to be solved that can greatly improve network security.

A. Coin Age

In the PeerCoin protocol block generation is based on *coin age* which is a factor that increases the weight of unspent coins linearly over time; the proof that has to be provided together with a new block and has to satisfy the following condition:

$$\text{proofhash} < \underbrace{\text{coins} \cdot \text{age}}_{\text{coin age}} \cdot \text{target} \tag{1}$$

The proof hash corresponds to the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time.

With this system it is possible for an attacker to save up enough coin age to become the node with the highest weight on the network. If the attack were to be malicious the attacker could then fork the blockchain and perform a double-spend. After this is done however, a second double-spend would require the attacker to save up coin age again, as the stake resets when the block was generated.

It is worth mentioning that this situation is highly improbable and that the incentive is questionable (saving enough coin age to be the highest weight on the network would either take a lot of time or a lot of coins, and thus money, to make this happen. Next to that, performing such an attack would probably devalue the system itself so it wouldn't be profitable to do the attack in the long run.)

Archived copy · cryp2nova.com

Another problem with coin age are greedy honest nodes. These are nodes that have no malicious intent but they keep their coins off the network and only stake every once in a while to get their stake reward. The current system actually encourages abusive behavior of these nodes by keeping their node offline until it accumulates enough coin age to get the reward in a short period of time and then shut down the node again.

B. Blockchain Precomputation and Long Range Attacks

At the time of writing of this paper there is no known solution for secure timestamping in a largely distributed network. The current block timestamp rules give an attacker a degree of freedom in choosing the proof hash described in Eq. 1 and therefore increase the probability of a successful attempt to fork from several blocks in the past.

In addition, the current stake modifier doesn't obfuscate the hash function enough to prevent the attacker from precomputing future proofs. An individual who is seeking to maliciously attack the network would therefore be able to calculate the next interval for the future proof-of-stake solutions, allowing that individual to generate a few blocks in a row and execute a malicious attack that could harm the network.

IV. Changes in the Protocol

In the following we will describe the changes in the POS protocol that address the problems described in the previous section.

A. Taking the Coin Age out of the equation.

The most secure way to perform a Proof of Stake system is by having as many nodes online as possible. The more nodes that are staking, the less possibility for security issues like 51% attacks, and the faster the actual network will perform transactions through these nodes.

Thus, taking out the coin age will require all nodes to be online more to get their stake reward. Saving up coin age is no longer a possibility with the new system that calculates the chance of staking as follows:

$$\text{proofhash} < \text{coins} \cdot \text{target} \tag{2}$$

Note that the system in Eq. 2 will not change the actual stake reward.

B. Changing the Stake Modifier

In order to mitigate the possibility of the pre-computation attack, the stake modifier will be changed at every modifier interval – to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake.

C. Block Timestamp Rules

Appropriate changes have been made to the block timestamps to work more efficiently with PoS. The expected block time was increased from original 60 seconds to match the granularity. Note that it is assumed that nodes have an external source of time, and if the internal time of a node deviates too much from the general consensus then there is a high probability that blocks generated by this node will get orphaned. The proposed changes below outline the modifications to the block timestamp rules.

Bitcoin	
Past limit:	median time of last 11 blocks
Future limit:	+2 hours
Granularity:	1 second
Expected block time:	10 minutes

okcash	(New rules)
Past limit:	time of last block
Future limit:	+15 seconds
Granularity:	16 seconds
Expected block time:	64 seconds

D. Hash Function

The original NovaCoin protocol called for the use of "Scrypt" [5] as its Proof-Of-Work; also being used as the block hash. However there are some issues with that previous implementation. Using Scrypt offers no real advantage to Proof-Of-Stake; and is far slower than some alternatives. Since Okcash is no longer in PoW phase, the only major change would have to occur in the algorithm for determining the block hash. Therefore the block hash has been changed back to SHA256d. To reflect this the block version has been increased to version 7.

V. Summary

The proposed changes are intended to improve security in Okcash's PoS protocol and were made with optimization in mind. With the new protocol possible attack vectors are reduced to a minimum and the incentive to support the network by having a full node running continuously is clearly increased. This will allow Okcash and PoS to continue to scale for mass adoption while plugging and mitigating potential risks.

VI. Acknowledgements

Many thanks to Oktoshi, Pavel Vasin, Rob 'Soepkip' Schins, Maarten Visser, Steven 'McKie' McKie and Patrick Doetsch for helping out with the writeup of the protocol v2 changes.

References

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

[2] Nicolas T. Courtois. On the longest chain rule and programmed self-destruction of crypto currencies, 2014.

[3] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013.

[4] NovaCoin. http://coinwiki.info/en/novacoin.

[5] Scrypt proof of work. https://en.bitcoin.it/wiki/scrypt proof of work.

[6] Okcash LTSS. https://github.com/okcashpro/okcash-whitepaper/blob/master/LTSS/okcash-long-term-staking-whitepaper.pdf

Archived copy · cryp2nova.com