Introducing Okcash v3 PoS LTSS

The Latest Advancement in Secure and Energy-Efficient Digital Currency

by Oktoshi

Abstract

The current state of Proof-of-Stake (PoS) protocols for digital currencies has several potential security vulnerabilities, such as coin age abuse by malicious nodes to gain significant network weight and perform successful double-spends, as well as the potential for honest nodes to abuse the system by staking only on a periodical basis, thereby undermining network security. Additionally, in current PoS systems, all components of the proof-of-stake are predictable enough to allow pre-computation of future proof-of-stakes. In this paper, we propose a new system, Okcash v3 PoS LTSS, that addresses these issues and improves network security and energy efficiency.

I. INTRODUCTION

The crypto-currency community has long recognized that Proof-of-Stake (PoS) has yet to fully prove its security, economic value, and overall energy efficiency over time. In light of this, we propose a new system, Okcash v3 PoS LTSS, that addresses these concerns and improves network security and energy efficiency.

This paper is organized as follows. Section II explains the benefits of PoS and its potential as a consensus mechanism for decentralized digital currencies. In Section III, we describe the flaws of current PoS implementations and their potential impact on network security. In Section IV, we present Okcash v3 PoS LTSS and its mechanisms for addressing these issues. Finally, in Section V, we provide a summary and discuss future research directions.

II. PROOF-OF-STAKE

Consensus in a decentralized digital currency like Bitcoin [1] is traditionally achieved through the use of a Proof-of-Work (PoW) mechanism, which requires generated blocks to contain a proof that the node which generated the block solved a computational hard task. However, PoW-based systems tend to be energy-intensive and have a limited lifespan [2].

PoS aims to replace the PoW mechanism as a method for achieving consensus in a distributed system. Instead of solving a computational task, a node that generates a block must show proof of ownership of a certain amount of coins, referred to as the "target," as specified by the network through a difficulty adjustment process similar to PoW. This process ensures an approximate, constant block time.

As with PoW, the block generation process is rewarded through transaction fees and a supply model specified by the underlying protocol, which can also be seen as an interest rate. 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 led to NovaCoin [4], which uses a hybrid PoS/PoW system. BlackCoin was the first cryptocurrency that used a pure PoS-based protocol, further enhancing the PoS system.

III. SECURITY ISSUES IN CURRENT POS IMPLEMENTATIONS

While PoS has several advantages over PoW as a consensus mechanism, it also has several unresolved problems that can greatly impact 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 must be provided together with a new block must satisfy the following condition:
$$proofhash < coins \cdot age \cdot target \quad (1)$$
The proof hash corresponds to the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time.

This system allows for the possibility of an attacker to save up enough coin age to become the node with the highest weight on the network. If the attack is malicious, the attacker could then fork the blockchain and perform a double-spend. However, it is worth noting that this situation is highly improbable, and the incentive for such an attack is questionable, as it would take a significant amount of time or coins to achieve a high enough coin age. Additionally, performing such an attack would likely devalue the attacker's own coins.

B. Periodical Staking

Another issue with current PoS implementations is that honest nodes can abuse the system by staking only on a periodical basis, rather than continuously staking their coins. This undermines the security of the network as it does not provide a constant level of security.

IV. OKCASH V3 PoS LTSS

To address the issues of coin age abuse and periodical staking, we propose Okcash v3 PoS LTSS. Our protocol implements several mechanisms to ensure network security and energy efficiency.

A. Randomized Staking

To address the issue of coin age abuse, our protocol implements randomized staking, which ensures that even if an attacker saves up a large amount of coin age, they will not necessarily have the highest weight on the network. This is achieved by randomly selecting the stake modifier, a variable used in the calculation of the proof hash, from a large pool of possible values.

B. Continuous Staking

To address the issue of periodical staking, our protocol implements a continuous staking mechanism, which requires nodes to continuously stake their coins to maintain their weight on the network. This ensures a constant level of security and prevents abuse of the system.

C. Dynamic Difficulty Adjustment

To improve energy efficiency, our protocol implements a dynamic difficulty adjustment mechanism, which adjusts the target difficulty level in real-time based on network conditions, rather than using a static difficulty level. This allows for a more efficient use of resources and reduces the risk of centralization.

D. Rate of Coin Creation

To further enhance the security of the PoS process, Okcash v3 PoS LTSS takes into account the overall expected rate of coin

creation and uses it in the calculation of the block reward formula: nSubsidy = (pindexPrev->nMoneySupply / COIN) * (RCOIN_YEAR_REWARD / 3) / (365 * 24 * (60 * 60 / 62.9138346197)) This calculation is done on each block of the OK chain, making it impossible for bad actors to modify or abuse this system in any way, while at the same time bringing more fairness to the overall staking system as it does not matter how many coins a user holds, they will gain rewards proportional to their exact coin weight.

E. Halving Periods

Okcash also implements halving periods [5] that further expand the security of the staking mechanism. These halvings occur at regular intervals and decrease the block reward, making it even more difficult for bad actors to exploit coin age or successfully attack the network. This, coupled with the other security and energy-saving measures implemented in Okcash v3 PoS LTSS, make it one of the most secure and energy-efficient proposals in the crypto space.

F. Increased Coin Confirmations

Okcash requires higher confirmation rates than most cryptocurrencies, making its transactions more secure. This is achieved by increasing the number of confirmations required before a transaction is considered valid.

G. Increased Block Speed

Okcash block time is 72 seconds, making the transactions relay virtually instant. This allows for faster confirmation of transactions and increased overall network efficiency.

V. CONCLUSION

In conclusion, Okcash v3 PoS LTSS offers a solution for a more secure, energy-efficient, and sustainable digital currency. By addressing the weaknesses of current PoS systems, our protocol ensures network security, promotes long-term growth, and achieves Bitcoin predictability under Okcash's unique LTSS PoS System. The protocol's combination of randomized staking, continuous staking, dynamic difficulty adjustment, rate of coin creation, halving periods, increased coin confirmations, and increased block speed, make it one of the most secure and energy-friendly proposals in the crypto space. We believe that this protocol can serve as a foundation for future research in PoS-based digital currencies.

References: [1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008 [2] G. O'Dwyer, D. Malone, and B. Donnelly, "Bitcoin Mining and its Energy Footprint," 2014 [3] Sunny King and Scott Nadal, "Peercoin: the secure and sustainable crypto-currency," 2013 [4] BCNova, "NovaCoin: a hybrid PoS/PoW cryptocurrency," 2013 [5] Oktoshi, “okcash-long-term-staking-whitepaper.pdf” 2014.