OduwaCoin's Proof-of-Stake Protocol
v2.0.0.0-IVIE

WHITE PAPER

WWW.ODUWACOIN.IO

https://oduwacoin.foundation/

Digital Cash

Abstract —

Over time, as blockchain consensus protocol becomes more familiar to the general public, the need for a secure Network with less complex incentivizing nodes operations for the decentralized market emerges.

The current Proof of Stake protocol has shown a significant market adoption but the effect on the network still poses several potential security issues. For instance, coinage can be abused by malicious nodes to gain significant network weight to perform a successful double spend.

Additionally, due to coinage, honest nodes can abuse the system by staking only on a periodical basis. The focus is security, scalability, and decentralization. The past protocol methodology does not secure the network. In the current system, all components of a stake of proof are predictable enough to allow pre-computation of future proof-of-stakes.

Lastly: Since network security depends largely on nodes participation and community incentivization, this implies that the future of blockchain adoption will be cultural to the problem the ecosystem is solving in a popularized community. Oduwacoin is the First-Indigenous-Pure-Pos- Cryptocurrency that is viable and alternative to bitcoin, designed to empower people of African descent. The network is designed to perform secure, scalable, and decentralized transactions. In the Oduwa blockchain network which is powered by its native cryptocurrency known as Oduwacoin, the incentive (ROI) for the miners is based solemnly on a yearly fixed decent reward, with less liability, and an inflation-proof mechanism.

Only 21, Million Oduwacoins will ever exist.

In this paper, IVIE Protocol is proposed to solve said issues.

I. INTRODUCTION

Proof-of-stake (PoS) blockchain protocols were envisioned as a solution to the immense energy demands of miner nodes in proof-of-work (PoW) based blockchain systems. PoS was proposed in discussions in the bitcoin forum, and it was adopted principle that the right to produce a new blockchain block should be awarded to a stakeholder with probability proportional to their current stake, as documented by the blockchain itself. Conceivably, such a blockchain discipline could yield desirable ledger properties without consuming significant real-world resources: no substantial energy expenditure would have to be invested to run the protocol. Such protocols would naturally replace the assumption of an honest majority of hashing power with the assumption of an honest majority of stake in the system. While the potential virtues of such PoS protocols are substantial, it was argued early on that the design of such schemes could be particularly challenging or perhaps even not feasible.

Currently, in the cryptocurrency community, it is a common understanding that Proof-ofStake has yet to prove its security, economic value, and overall energy efficiency over time. Oduwacoin is designed to prove that the concept of Proof-Of-Stake is valid; insisting it connects with real people and has real-world applications in the future of cryptocurrencies.

As we expect the Oduwacoin ecosystem to grow in the future, we want to ensure that the Proof-of-stake system is as secure as it can be. Therefore, we will be introducing PoS Protocol IVIE also known as Oduwacoin.v2.0.0. IVIE.
In the future, we will continue to expand and reinforce the new system with a bullet proof network
This version will highlight a critical step in our journey to deliver blockchain applications that directly connect to real people, particularly those informed by the indigenous community.

Section II explains the importance of the Proof-of-Stake concept.
In Section III we describe the flaws or bugs of the current implementation which are then addressed in Section IV.
Finally, we give a summary in Section V.

II. PROOF-OF-STAKE

Consensus (PoS) is a consensus algorithm for blockchain networks that relies on randomly selected validators, who "stake" the native network's asset by locking them into the blockchain, to produce and approve blocks.

Validators are rewarded based on their total stake, incentivizing nodes to validate the network based on a return on investment (ROI).
PoS is largely viewed as the greener, and more scalable version of Proof of Work (PoW) consensus in Bitcoin [1], which requires significant energy expenditures to achieve its goal by requiring generated blocks to contain proof that the node which generated the block solved a computationally hard task.

Unfortunately, the concept of the Proof-of-Work (PoW) based system tends to lean towards eventual self-destruction. The main disadvantages of PoW are the **huge costs of computing and mathematical calculations, 51% attack. Huge expenses**. To solve PoW problems, expensive and highly specialized computer equipment is needed. I mean your money should work for you and not against you.

[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 must provide proof that it has access to a certain number of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required number 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 except no transaction fees and a supply model specified by the underlying protocol, which can also be an interest rate by common definition. The initial distribution of the currency is usually obtained through a period of PoW mining. A. Related work 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 adopted by Oduwacoin and then BlackCoin which tends to fix many securities issues in Pos Network similar to Oduwacoin's Network improvement called IVIE

Oduwacoin is the First Indigenous Cryptocurrency that uses a pure PoS protocol that is based on the development of the above-described projects but directly connects to real people.

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 must be provided together with a new block and must satisfy the following condition:

$$\text{proof hash} < \text{coins} \cdot \underbrace{\text{age}}_{\text{coin age}} \cdot \text{target} \quad (1)$$

The proof hash corresponds to the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. With most protocols in the market, an attacker can save up enough coinage 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 coinage 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 coinage 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 would not be profitable to do the attack in the long run.) Another problem with coinage is greedy honest nodes. These are nodes that have no malicious intent, but they keep their coins off the network and only stake occasionally, to get their stake reward.

The old system encourages abusive behavior of these nodes by keeping their node offline until it accumulates enough coinage to get the reward in a short period of time and then shut down the node again.

B. Blockchain Precomputation and Long-Range Attack

At the time of writing this paper, there is no known solution for secure timestamping in a large, 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 does not 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.

One particularly critical threat in the PoS setting was documented by Buterin [But14] who referred to it as the problem of "long-range attacks" (also related to the concept of "costlesssimulation" in, e.g., [Poe15]). This refers to the ability of a minority set of stakeholders to execute the blockchain protocol starting from the genesis block (or any sufficiently old state) and produce a valid alternative history of the system. Confronted with such alternative history and no other outside 1See e.g., the post by user QuantumMechanic https://bitcointalk.org/index.php?topic=27787.0 and the ensuing discussion in 2011. information beyond the genesis block, a freshly joining node would have no ability to reliably distinguish between this alternate history and the actual history. It follows that with such an attack a minority set of stakeholders could doublespend or erase past transactions, violating the fundamental persistence property of the resulting ledger. In the same blog post [But14], however, a glimmer of hope was also provided: it was observed that the blockchains produced by such a minority set of stakeholders may have characteristics that could be used to distinguish them from the actual blockchain maintained by the honest majority. If timestamps are included in each block, it would be the case that a simple simulation of the protocol by a minority set of stakeholders would result in a blockchain that is sparse in the time domain and, as a result, a longest chain rule at any particular moment would favor the blockchain produced by the honest parties

IV. CHANGES IN THE PROTOCOL

In the following, we will describe the changes in the Oduwacoin 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 coinage will require all nodes to be online more to get their stake reward. Saving up coinage is no longer a possibility with the new system that calculates the chance of staking as follows:

proof hash < coins · target (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 the 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 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

Oduwacoin (New rules)

Past limit: time of last block

Future limit: 10 Minutes

Granularity: 16 seconds

Expected block time: 120 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.

One of the central pillars of any cryptocurrency is the hashing algorithm it is based upon, but what makes these algorithms important, and what are the differences between each algorithm?

You may be asking yourself, who chooses the algorithm for a cryptocurrency?

The chosen algorithm is up to the coin's development team, not the miner; there are many reasons why the chosen algorithm was implemented, ranging from long-term goals to network security, and even protection from ASIC mining hardware. It is important for miners to consider the algorithm of a coin they are willing to mine for several reasons, including the electricity required to mine, the effectiveness of their existing hardware on the network, and whether they wish to mine with GPU, CPU or ASIC based mining equipment.

What makes each hashing algorithm unique is often most important to the coin developer, for instance, SHA-256 based coins have a block time of around 8-10 minutes, whereas Scrypt coins can have block times as low as 30 seconds.

Using Scrypt offers has real advantage to Proof-Of-Stake at the earlier stage of pre-mining.

Scrypt requires attackers to either use more memory to conduct a brute force attack, or use less memory and conduct a slower attack, this tradeoff is intentional and makes Scrypt very secure. It is no wonder it was first implemented by Litecoin creator Charlie Lee as the coin's algorithm. Since Oduwacoin is no longer in the PoW phase, the only major change would have to occur in the algorithm for determining the block hash. Therefore, the block hash remains Scrypt. The proposed changes IVIE are intended to improve security in OduwaCoin'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 Oduwacoin and PoS to continue to scale for mass adoption while plugging and mitigating potential risks.

Coinomics

PROTOCOL: IVIE

Coin Name: OduwaCoin

Ticker: OWC

Decimal: 8

Block Time: 120 sec.

Last PoW Block: 5000

Algo: Scrypt

Maturity: 20 blocks

Min. Stake Age: 8 hrs

StakeSplitThreshold: 1000

RPCPort: 26682

Port: 26681

MAX SUPPLY: 21 MILLION

Epilog

Oduwacoin is the future of money.

Digital Cash

Indigenous

Blockchain Culture

Qualities of Oduwacoin

A. Scarcity

B. Divisibility

C. Fungibility

D. Limited Supply

E. Portability

F. Immutability

G. Homogeneity

H. Globality

VI. ACKNOWLEDGEMENTS

Many thanks to Bright Enabulele, Charles Anchang, for putting together a write-up and review of Oduwacoin protocol v2.0.0 IVIE 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 selfdestruction of cryptocurrencies, 2014. [3] Sunny King and Scott Nadal. Popcorn: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013. [4] Novocoin. http://coinwiki.info/en/novacoin. [5] Scrypt proof of work. https://en.bitcoin.it/wiki/scrypt proof of work [6] Stake-Bleeding Attacks on Proof-of-Stake Blockchains (nsf.gov) [7]Blackcoin [8] Crypto Mining: SHA-256 or Scrypt – A Guide for Miners -Bank Manager[9] litecoin