Nodium Technical Whitepaper:

Beta Version: 1.0

www.nodium.org

Date: 16th April 2018

The technical notes in this document describe the features of Nodium cryptocurrency and detail the specifics of POW/POS rewards system. This is our Beta whitepaper in a basic format and will be updated in due course as the Nodium project progresses.

Abstract: The current widely used proof of stake protocol has a several potential security issues. The lack of digital currencies offering private transactions poses risk for exposing of transactions to third parties. In addition, proof of work focused cryptocurrencies offer risk on computational power being eventually owned by large companies and individuals which can put the network at risk. In this paper, Nodium aims to propose a solution to these issues.

1. Nodium Introduction

Nodium is a community and privacy focused cryptocurrency based on a POW/POS hybrid system. Nodium utilizes the masternode and staking based algorithm in it's primary long-term use case, focused on creating a secure network which is decentralised across a large user base of nodes not owned or maintained by a single party. This ensures the network stays decentralised and has no controlling ownership, decisions for the cryptocurrency are made via community governance, unlike most current financial world currencies.

Related work:

The first POS cryptocurrency was PeerCoin. Further development built upon this was NovaCoin which uses a hybrid POS/POW system. After which developed further creating such cryptocurrencies as PIVX also utilising the same algorithm model. BlackCoin is the first pure POS coin.

1b. Nodium POS Explained

POS (proof of stake) allows a holder of cryptocurrency on the Nodium chain to validate transactions on the chain according to the amount he/she holds. Simply put, the more coins held, the more transactions are validated (or mined) by the holder. POS eliminates the need for miners on the network to validate transactions. The first cryptocurrency to adopt the POS method was Peercoin, after which other forks have been adapted upon.

Eco Friendly:

Proof of stake is a much more eco friendly method of validating transactions on a network, as it requires much less power compared to a standard mined cryptocurrency. Mining requires a great deal of power to run it's cryptographic calculations. It was estimated that 1 bitcoin transaction required 1.57 American households per day in 2015, and as a result miners would usually part sell awarded coins for fiat currency to pay for electricity costs on mining, which in turn defeats the use case of a cryptocurrency as a useable world currency.

1c. The problem and solution

POW Negatives:

Cryptocurrencies relying solely on the POW system are susceptible to a potential tragedy of commons. This refers to a future point in the cryptocurrency landscape where potentially there are fewer miners available due to little/no block reward from mining. The only fees being in the future from validating transactions. When fewer miners are required for mining coins, it puts the network under vulnerability to a 51% attack. This happens when a miner/mining pool controls more than 51% of the computational power and creates fraudulent transactions for him/herself while invalidating transactions for other users on the network.

POS Positives:

With a POS based algorithm, the attacker would need to obtain 51% of the cryptocurrency to carry out a 51% attack. A proof of stake network avoids this by making it disadvantageous or a miner with 51% stake in the cryptocurrency as it's almost firstly near impossible to obtain such a large stale in the network and it would not be in the interest to attack a network he/she holds in the network as it would affect the value of holdings. Simply put for an attack to happen, it's much less likely as POS does not rely solely on computing power from miners, instead it's users staking their currency for rewards.

2. Nodium POS/POW consesus and block rewards

Nodium will allow POW for the first stage of the cryptocurrency to allow fair use for miners to mine the coin early on, which helps distribute it throughout the community and exchanges. After this block period is finished, POS will activate and be the only transaction validation work the currency uses. Below are the block reward periods explained:

3. Reward Distribution

Please refer to our GitHub Nodium coin repository for exact specifications.

5. Proof of stake 2.0 overview

To achieve consensus proof of stake requires nodes running a wallet in order to prove it has coins on the network. The participating wallets then receive part of the block reward proportional to the amount of coins staked.

The benefit of this protocol is that is results in a high amount of nodes on the network making it more secure than a conventional POW based coin which relies on computing power.

Holders of XN (Nodium ticker) will be able to stake from their wallet and receive a reward for helping to participate with transaction verifications on the network.

6. Masternodes Overview

Masternodes are also nodes running on a wallet via a server, however require a larger amount of coins to provide extra services on the network. Nodium requires 10,000 XN. These services will include coin mixing for increased privacy of transactions, instant transactions and decentralized governance which provides a budgeting system for proposals on the Nodium chain.

Holders of masternodes will receive a larger reward, and this can serve as a passive income. (Rewards can be seen on our whitepaper rewards section)

7. ZeroCoin Protocol:

ZeroCoin allows for coin-mixing with zero knowledge transactions to be made on Nodium. This means that every XN transaction using ZeroCoin is 100% private as has no prior transaction history attached to it. You can find out more about the ZeroCoin feature on our separate whitepaper. This feature is planned to be added Q3 2018.

8. Project goals

8a. Short term

- *Secure network*
- *Strong community core*
- *Social network popularity*
- *Governance*
- *Masternodes and staking*

8b. Long term

- *Wide scale use case*
- *Smart contracts*
- *Card/App payment system*
- *Decentralized exchange*
- *Decentralized marketplace*
- *1000+ masternodes*

Conclusion:

Nodium aims to help bring cryptocurrency to a larger audience, and maintain it's use case as a community driven project with developers and supporters at its core. Private transactions and speed are a primary focus for the project. Nodium aims to represents a real world sustainable use case in the long term view of blockchain and using cryptocurrency as a form of payment.

references:

https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf

https://peercoin.net/assets/paper/peercoin-paper.pdf

https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

https://altcoinwiki.org/en/Novacoin