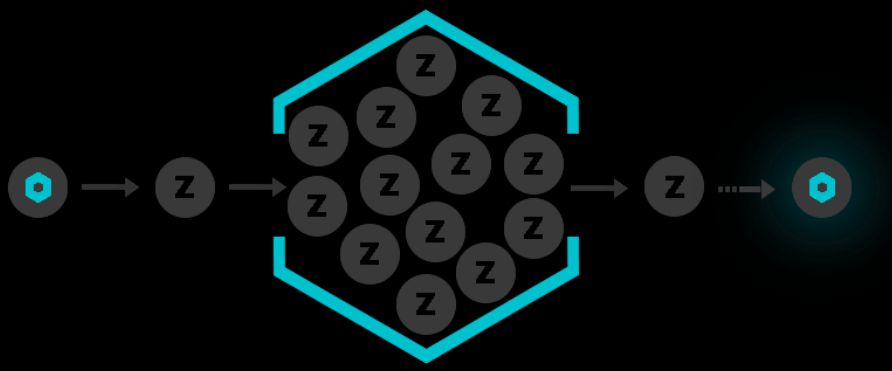
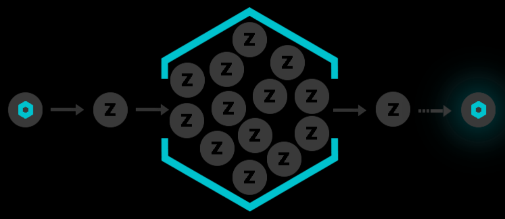
Nodium



Powered by Masternodes.

Technical Whitepaper V1.4

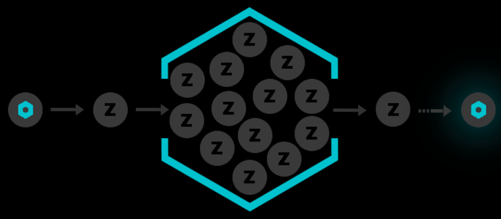
Introduction



Nodium is a community and privacy focused cryptocurrency based on a POW/POS hybrid system. Nodium utilizes a masternode and staking based algorithm in its 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, and decisions for the cryptocurrency are made via community governance, unlike most current financial world currencies.

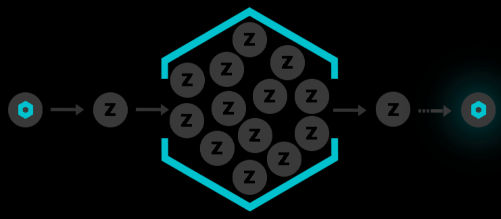
Masternodes provide the backbone to the network security, for this they are rewarded 90% of the block reward, while staking partners receive the remaining 10%. We believe this provides sufficient incentive to participate while reducing volatility and delivering a stable currency.

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.

Nodium PoS

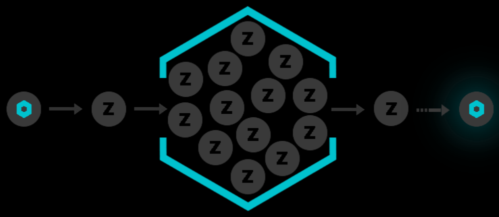


POS (proof of stake) allows a holder of cryptocurrency on the Nodium chain to validate transactions on the chain according to the amount he/she holds. Simply put, the more coins held, the more transactions are validated (or mined) by the holder. POS eliminates the need for miners on the network to validate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

Environmentally efficient

Proof of stake is a much friendlier method of validating transactions on a network, as it requires much less power compared to a standard PoW cryptocurrency. Mining requires a great deal of power to run its 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.

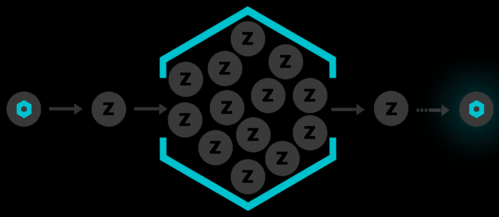
The Problem – The Solution



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.

Specifications



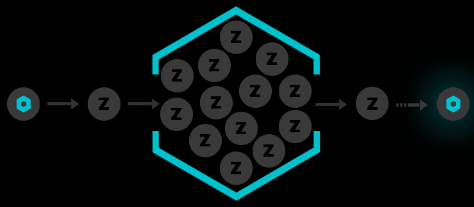
Algorithm	Quark
Block Time	60 Seconds
Difficulty Retargeting	Every Block
Max Coin Supply (POW Phase)	49,750
Max Coin Supply (POS Phase, pre Infinite)	30,259,115 XN
Premine	4,000,000 XN
Block Maturity	60 Minutes
Masternode Collateral	10,000XN

Reward Distribution

Phase	Block eight	Reward	Masternode	Staking
Phase 1	201-50000	200 XN	90% (180 XN)	10%
Phase 2	50001-75000	150 XN	90% (135 XN)	10%
Phase 3	75001-100000	100 XN	90% (90 XN)	10%
Phase 4	100001-150000	75 XN	90% (67.5 XN)	10%
Phase 5	150001-200000	50 XN	90% (45 XN)	10%
Phase 6	200001-250000	30 XN	90% (27 XN)	10%
Phase 7	250001-300000	15 XN	90% (13.5 XN)	10%
Phase 8	300001-400000	10 XN	90% (9 XN)	10%
Phase 9	400001-500000	5 XN	90% (4.5 XN)	10%
Phase X	500001-Infinite	5 XN	90% (4.5 XN)	10%

$$Daily\ Reward = \left(\frac{nodesOwned}{nodesInNetwork}\right) * (BlockReward * BlocksPerDay * Reward\ \%)$$

PoS 2.0



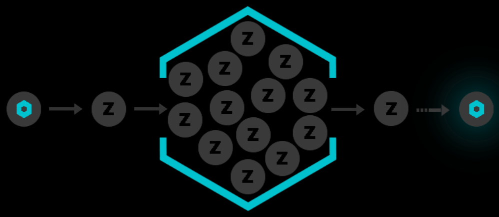
To achieve consensus proof of stake requires nodes running a wallet in order to prove it has coins on the network. The participating wallets then receive part of the block reward proportional to the amount of coins staked for helping to participate with transaction verifications on the network.

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.

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 above in the rewards section)

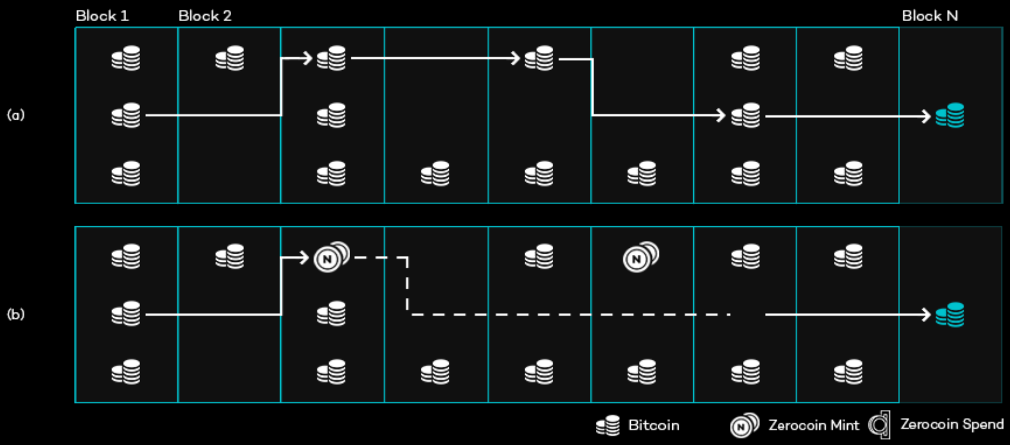
Bitcoin is not Private



The Bitcoin payment network offers a highly decentralized mechanism for creating and transferring electronic cash around the world. Unfortunately, Bitcoin suffers from a major limitation: since transactions are stored in a public ledger (called the “block chain”) it may be possible to trace the history of any given payment — even years after the fact. Worse, since the Bitcoin ledger is public, any party can recover this information and data mine to identify users and patterns in the transactions. In other words: Bitcoin transactions are conducted in public.

The Bitcoin protocol and clients address this in two ways: (1) all Bitcoin transactions are conducted using public keys as identifiers, and these public keys are not linked to individual names. And (2) Bitcoin clients are capable of generating many public keys (“identities”) to help users resist tracking. Unfortunately, a growing body of research indicates that these protections are insufficient. This information may allow data miners to link individual transactions, identify related payments, and otherwise trace the activities of Bitcoin users.

ZeroCoin Protocol



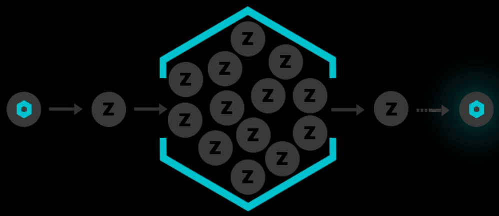
Zerocoin is a project to fix a major weakness in Bitcoin: the lack of privacy guarantees we take for granted in using credit cards and cash. Our goal is to build a cryptocurrency where your neighbors, friends and enemies can't see what you bought or for how much.

This project began with a proposed extension, called "Zerocoin", to the Bitcoin protocol that allowed users to mix their own coin. A collaboration between the original Zerocoin project members and cryptographers at MIT, The Technion, and Tel Aviv University, has produced a far more efficient protocol that allows for direct private payments to other users of hidden value.

How Zerocoin works

The Zerooin protocol allows direct anonymous payments between parties. Zerocoin transactions exist alongside the (non-anonymous) Nodium currency. Users can convert (non-anonymous) coins into (anonymous) coins, which we call zerocoins. Users can then send zerocoins to other users, and split or merge zerocoins they own in any way that preserves the total value. Users can also convert zerocoins back into XN.

Roadmap



Smart contracts

Card payment system

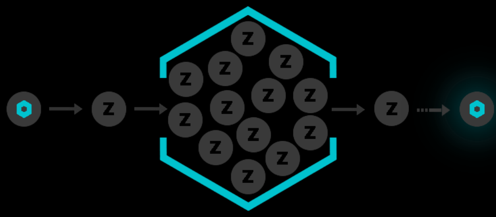
Mobile Wallets

Decentralized exchange

Decentralized marketplace

1000+ Masternodes

Conclusion



Nodium aims to help bring cryptocurrency to a larger audience, and maintain its 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

http://www.zerocoin.org