# **Blockchain Core**

# **1 Basics**

A table with an overview of the support status and applicability.

|  |  |
| --- | --- |
| Status: | e.g. **Supported**/**Tech Preview**/**Experimental** |
| Architecture(s): | e.g. mesh network |
| Component(s): | e.g. PIVX, Name Coin |
| Hardware: | *where applicable* |

# **2 Overview**

**Obfuscation**

Mixing Mechanism: In wallet coin mixing based on CoinJoin with various improvements over the original, but done in a decentralized fashion facilitated by the network of masternodes. This provides for an additional layer of privacy in transactions, while not perfectly anonymous, it is a far cry better than the standard bitcoin transaction. If a nefarious actor were to control 50% of the current masternodes, they would have less than 0.5% chance of de-anonymizing an individual transaction that was mixed with eight rounds of Obfuscation.

**SwiftTX**

Instant Transactions: SwiftTX transactions are confirmed and spendable within seconds, guaranteed by the network of masternodes, with no need to wait for multiple confirmations to be confident in the validity of the transaction.

**Code Base: PoS 3.0 Bitcoin Core 0.10.x**

PIVX is the first proof of stake cryptocurrency to be based on the version 0.10 or higher Bitcoin codebase, and the PoS structure utilised does away with coin age, meaning in order to get the most out of your staking you must keep your wallet open at all times, resulting in more constantly available nodes, strengthening the network. No more users were opening their wallet once or twice a month for a few minutes and getting rewarded equally with those that have 24/7 up-time with their wallet.

**See-Saw Rewards Mechanism**

Block rewards received by the staker and winning masternode vary based on the number of coins held for masternodes vs. amount of coins available for staking on the network allows for Variable rewards based on needs of the network to keep the network services (Masternodes) and the security of the network (Staking Wallets) evenly distributed. When there are fewer as the number of masternodes rises the portion of the block reward that they earn is reduced, it increases when the number of masternodes declines.

**Masternodes**

These are incentivized nodes that receive rewards based on their availability and their ability to offer network services in a decentralized and trust-less manner. Running a masternode requires locking 10,000 PIV collateral for as long as you choose to run the masternode and allows the owner to vote on budget and development proposals. These nodes are the backbone of the present, and future services offer on the PIVX network, and as such are rewarded at a slightly higher level as compared to just staking when the number of them is at a predetermined level defined in the seesaw mechanism.

**Decentralized DNS**

This would avoid domain name censorship by making a new top-level domain outside of ICANN control. The coin is designed to halve every four years with the same cap limit as Bitcoin of 21,000,000. With the domain registry service, a small number of NMC will be destroyed so after mining has finished there will still be a deflationary element in place. Namecoin was the first coin to switch to merged mining.

# **3 User details**

**User registration**

The registration fee is ??? DIVI, and the transaction fee is determined dynamically by miners (just like in Bitcoin). The registration fee might be made dynamic in the future, to improve economic incentives.

# **4 Technical details**

Information for a developer or power user. Should include where to look in-tree for detailed documents and code.

# **5 Limitations**

**DNS feature**

You have to renew or update a name every 35,999 blocks at the latest (between 200 and 250 days); otherwise, it expires. There are no registration fees for renewals or updates, but a transaction fee does apply.

# **6 Testing**

A side-chain test network environment will be necessary to gauge actual transaction times, block times, block height, staking vs. masternode rewards based on the see-saw algorithm, and one-click installation on both desktop and VPS.

# **7 Areas for improvement**

List of enhancements which could be undertaken, e.g. to improve the feature itself, or improve interaction with other features.

# **8 Known issues**

The pricing algorithm wasn’t very sophisticated. As a result, there was a lot of spam registrations on Namecoin. There is a paper that came out by Arvind [Narayanan], the professor at Princeton, and they analyzed how much spam registrations there are -- and I think the results were shocking. I think less than 1 percent of names on the .bit namespace currently map to anything meaningful.

Because Namecoin was an old fork and it didn’t keep up with all of the development that was happening with Bitcoin, the software was lacking stability, as compared to Bitcoin. The ecosystem of how many developers are working on Namecoin was much smaller than the number of developers working on Bitcoin.

A security issue where it turns out that Namecoin does merge mining with Bitcoin, so basically, some miners would mine both cryptocurrencies because it is the same hash that they’re calculating and they can get rewarded on two different chains.

# **9 References**

**Namecoin**

<https://namecoin.org>

**PIVX**

<https://pivx.org>

<https://github.com/PIVX-Project/PIVX>