TECHNICAL NOTES

Seesaw Reward Balance System

Whitepaper

Revision 0.7e
January 24 2017
pivx.org

These technical notes are intended to formally document and describe the features and concepts of the Private Instant Verified Transaction cryptocurrency. This specific document will thoroughly explain in detail the technical details of the Seesaw Reward Balance System along with its intended benefits.

INTRODUCTION

The majority of crypto currencies that make use of masternodes, split their block reward per block equally between the mining and masternode distribution mechanisms. The intended fairness of this reward distribution can be subverted by the growth of masternodes held by large investors without limits leading to potential centralization of the budgeting system much like having a majority shareholder in a company. The additional benefits of masternodes can lead to less number of users conducting Proof of Stake (PoS) mining activities and thus lowering the security of the PoS network.

Masternodes do provide a valuable service and should be rewarded for that service, but our aim here is not to reward them way beyond the extra value they provide. For we believe that doing so disproportionately benefits masternode owners above and beyond other users of the system and ultimately leads to a greater degree of centralization.

To overcome this problem, the feature outlined in this paper was developed and implemented with the sole intention of ensuring the security of the PoS network. This is achieved by creating an incentive to stake, which subsequently promotes liquidity in exchanges and controls the growth rate and count of the masternode network.

PIVX OVERVIEW

Private Instant Verified Transaction, PIVX, is a privacy focused decentralized open source cryptocurrency launched in January 30th 2016 under the name of Darknet (DNET) before it was professionally re-branded to PIVX. Initial Proof of Work (PoW) distribution phase ended August 2016 when DNET transitioned to the current Proof of Stake (PoS) phase.

PIVX runs on a custom implementation of Blackcoin PoS 2.0[1] protocol on its Bitcoin core 0.10.x core and is a fork of DASH v0.12.0.x. It utilizes a network of masternodes[2] for an openly visible decentralized governance and increased transaction privacy.

The main goal of PIVX is to achieve near instant private transactions and a governance that helps sustain the network for the benefit of all of the users involved. While we are well on our way to achieving this, some of the features are under development and should appear in the near future.

PIVX has an open task and development environment and a highly accessible development team utilizing multiple social networking channels, including social media. The development team is welcoming of anyone and everyone to join its cause, regardless of technical expertise. We encourage people to just go ahead and do things rather than having lots of gatekeepers or a hierarchical structure where permissions are required to move forward.

For more specific details on PIVX, please visit pivx.org.

PROOF OF STAKE 3.0 OVERVIEW

To achieve consensus; Proof of Stake 3.0 (PoS) requires nodes running a wallet software proving that it has coins in the blockchain in order to verify a block of transactions. The participating nodes receive an amount of blocks proportional to their stake per set period as a form of reward.

This means that with lots of participating nodes (with roughly even amounts of coins) the network becomes very secure due to the increased difficulty of owning a majority of coins in the network.

MASTERNODES OVERVIEW

Masternodes are nodes running the same wallet software on the same blockchain to provide extra services to the network. These services include coin mixing for increased privacy of transactions, instant transactions and a decentralized governance that provides a decentralized budgeting system with immutable proposal and voting systems.

For providing such services, masternodes are also paid a certain portion of reward for each block. This can serve as a passive income to the masternode owners minus their

running cost.

MAIN FEATURE OVERVIEW

To promote an even ratio between staking nodes and masternodes in the network, the PIVX team has developed a variable Seesaw Reward Balance System that dynamically adjusts its block reward size between masternodes and staking nodes.

Each PIVX PoS block reward is split with 10% dedicated to the budgeting system and 90% dedicated to both the masternodes and stake mining reward. The reward portion is further split dynamically via the Seesaw Reward Balance System between masternodes and staking nodes.

The logic is simple in its roots. The higher the masternode count, the smaller the reward portion of each PoS block that will be paid out to the masternodes and the larger the reward portion for staking nodes. Conversely, when the masternode count falls, the masternode reward portion is increased and the staking node reward portion decreased.

The PoS block reward starts with a ratio of 9 to 1 towards masternodes when the amount of coins locked to masternodes is lower than 1% of the total coin supply.

But as the number of coins locked to masternodes go above 41.5% of the total PIVX coin supply, the block reward amount will shift with more than 50% of the block reward going to staking nodes. This has the effect of making it less attractive to provision more masternodes as it has the potential to significantly lower its profitability compared to staking that has less upkeep cost.

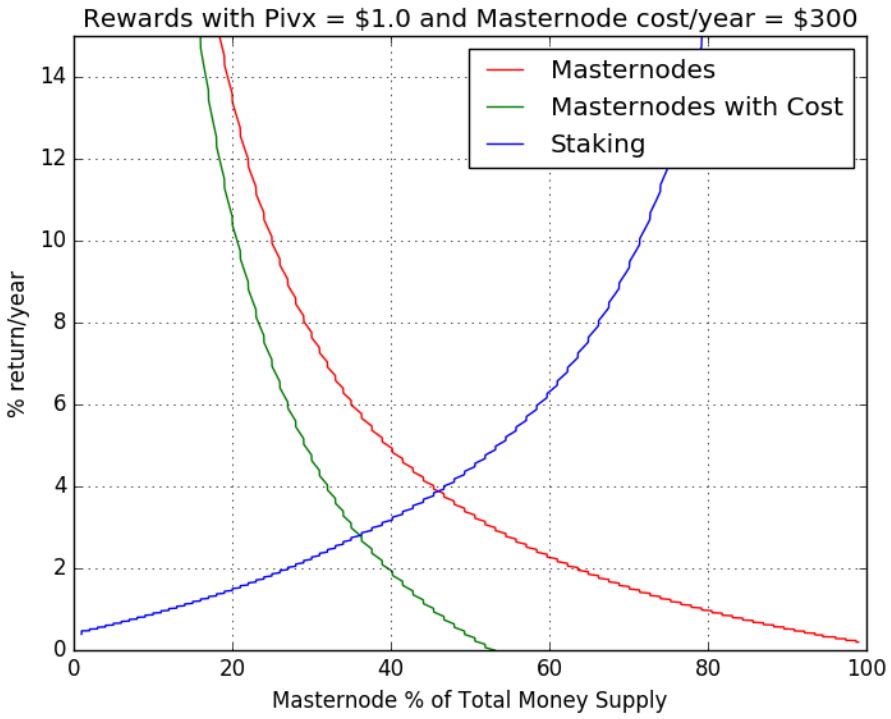
This threshold was selected as it would allow a strong network of profitable masternodes while creating incentive for approx. 60% of the total coin supply to be available for staking to secure the network and to maintain liquidity.

Another intended benefit and goal of the Seesaw Reward Balance System is to ensure that it is more profitable for users running masternodes than it would be to stake the equal number of coins, under the normal circumstances of being below the equilibrium threshold. The reason behind this is due to the extra cost, risk and time associated with maintaining the masternodes are greater than staking alone.

SEESAW EFFECT

Following graph shows the block reward amount (Y axis) for the masternodes (RED) and staking nodes (BLUE) against the percentage of total coin supply locked by masternodes (X axis) starting from block 648,000 (mid-May 2017) where each block rewards is fixed at 5 PIV.

Following graph shows the their theoretical annual percentage return starting from block 648,000 where each block is fixed at 5 PIV with an interval of 60 seconds. (1440 blocks a day)



The RED line represents the return of masternodes when there is zero upkeep cost per masternode and GREEN line is the logical masternode return curve on a hypothetical scenario where there is an annual upkeep cost of $300 per masternode with the price of each PIV at $1 USD.

The BLUE line represents the % return per year calculation of staking nodes is based on the assumption that all remaining coins are being staked. So the actual return rate for staking nodes may vary depending on how many are being staked at any given point in time.

CODE LOGIC WALKTHROUGH

The logic is intended to be simple as possible while being effective. This is to ensure its stability and to be able to easily determine its outcome and improve its logic if the need arises. This logic is run every block meaning it balances its block reward every 60 seconds.

```
if (mNodeCoins <= (nMoneySupply * .01) && mNodeCoins > 0) {
        ret = blockValue * .90;
    }
```

The *blockValue* is the total number of coins per block. This value is multiplied by the variable ratio that is determined by the percentage of the masternode coins, (*mNodeCoins*) in relation to the total coin supply (*nMoneySupply*). The result ret value is the number of coins for the masternodes portion of the reward.

Above example shows the very first logic used to determine the highest masternode portion payout. You can see that if *mNodecoins* is less than or equal to 1% of the coin supply (*nMoneySupply*) and also greater than 0, the return block reward value for the masternode will be 90% of the PoS block (*ret = blockValue * .90*).

This logic continues for each increase in set percentages all the way until *mNodeCoins* is less than or equal to 99% of the coin supply.

```
else if (mNodeCoins <= (nMoneySupply * .99) && mNodeCoins > (nMoneySupply *
.987)) {
        ret = blockValue * .05;
    }
```

Any *mNodeCoins* value that is beyond 99% of the total coin supply will return a fixed value equal to 1% of the *blockValue*. The expectation is that it should never come to this point but the logic is complete to cover all possible outcome.

```
else{
        ret = blockValue * .01;
}
```

This Seesaw Reward Balance System algorithm initially started out with only 16 percentage steps; it has since been improved and now implements a total of 105 percentage steps to the variable seesaw algorithm that allows for a far more granular

step amount.

SUMMARY

The Seesaw Reward Balance System that PIVX utilizes, provides numerous benefits over reward split methods used by the majority of masternode featuring Proof of Stake crypto-currencies.

1. It can indirectly affect the total count of masternodes in the network by varying its reward size to alter its profitability versus staking.

2. Promotes staking by increasing its reward payment portion when masternode count is high and thus maintaining a high level of network security.

3. Profitability of masternode is kept higher than staking as long as the masternode count remains below the equilibrium threshold. (Approx. 40% of coin supply)

4. Allows all coins owners to get rewarded for holding coins rather than just the masternode owners, hence resulting in a fairer and less centralized system

FUTURE PLANS

As the Seesaw Reward Balance System is still relatively new (only 5 months old at the time of writing this document); fine tuning may be required as the network grows and if better thresholds are deemed more effective.

But even within the first 5 months of PoS with over 1400 masternodes that make up over 30% of the current coin supply; the algorithm has been proven to work seamlessly as designed.

SOURCE CODE

GITHUB
https://github.com/PIVX-Project/PIVX/blob/6700079eed972831bd55179c029f0a2481e255f1/src/main.cpp#L1741

LINKS

BCT ANNOUNCE THREAD
https://bitcointalk.org/index.php?topic=1262920.0

Official Website
https://pivx.org

Masternode Payment Information
http://178.254.23.111/~pub/DN/DN_masternode_payments_stats.html

REFERENCE

[1] PoS 2.0 Whitepaper
http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper-cn.pdf

[2] DASH Masternodes
https://dashpay.atlassian.net/wiki/display/DOC/Masternode

AUTHOR

Written by: jakiman
Edited by: werwortmann, spock