**Tango**

**Abstract**

A proposal to expand representation in the PIVX governance system to include masternodes and stakers by leveraging the existing block reward distribution system.

**Introduction**

As we’ve already voted in favor of the distribution of voting power and the categories of proposals, the focus of this proposal will be an idea for the distribution of that voting power. This proposal expands representation in PIVX governance to stakers, a group with a 0.1 piv minimum rather than 10,000 piv.

**Goals**

In my view, the governance system of PIVX should maintain our core principles and features like privacy, decentralization, and security. As is referenced in the manifesto, these are non-negotiable. The voting system should not encourage frivolous blockchain activity or compromise the robust nature of the PIVX network.

It should be easy to vote and the system should be easy to understand. There seems to consensus on this point for any future governance system, so the complexity of a potential GUI voting interface and proposal list should be considered.

Voting weight should, to some degree, scale with the voter’s investment in the network. This is appropriate based on some investors having more to gain or lose, but also protects against sybil-type attacks on the governance system.

The system should be transparent, but maintain privacy. Voting should be as democratic as technologically possible. The system should value those who help PIVX and users should be incentivized to vote in PIVX’s best interest.

**Distribution of the Vote**

PIVX already has a decentralized, private, transparent, secure, robust, and streamlined mechanism and it already belongs to the masternodes and stakers. The PIVX block reward system meets all these goals and since it is an existing system, the vote distribution would not be anything additional for the user to understand. The block reward system is already well-tested as a security and incentive mechanism, so it is known to be secure and aligns with beneficial network participation.

I propose that we adapt the existing reward system to distribute voting rights and weight. In this proposal, voting weight will be referred to as tickets only for tangibility. To clarify, they would not be a new token, blockchain, ledger, or otherwise additional system for the network. Voting tickets would not really exist on a technical level, so there is not a requirement for much complexity, storage, or bandwidth.

In this new system, you would get voting tickets at a 1:1 ratio to your piv rewards from masternodes and staking. If you get 6.3 reward piv during a cycle, you would also get 6.3 voting tickets. Similar to the current voting system, your entire voting weight is valid for each proposal, so strategic vote rationing is not a factor.

Each cycle (~30 days), there are 43,199 blocks, 86,398 rewards, and 388,791 new piv awarded, and therefore 388,791 voting tickets available per cycle. The seesaw algorithm will also apply to the voting ticket distribution, which makes the system harder to exploit. This means some cycles masternodes may get more or less tickets than stakers.

**Implementation**

As mentioned, there is no actual voting ticket to hold or redeem. This approach will adapt the current system of masternode voting by signing votes with an address, but expand it to staking addresses. The PIVX network will accept signed votes and weigh their votes according to the block rewards from the current cycle (43,199 blocks). There is no need to trust the voter about their vote weight.

For example, if Bob wants to vote he can review open proposals in his wallet and then cast the vote Yes or No for each proposal. The wallet will prompt him for his passphrase, similarly to sending a transaction, and then transmit his votes to the network for any addresses that won a reward during the last cycle. The unlock is required because the wallet would be using his private key to sign each message with his vote and address. The PIVX network would then scan the blockchain back to the last superblock to validate the amount of reward piv that address won during the cycle, and weigh that vote accordingly.

**Approval Threshold**

In this ticket system, there are 388,791 voting tickets available each cycle. All votes would be pooled together and be subject to an approval system similar to the current one. The current approval threshold is 50.1%, with at least 10% possible votes. In other words, a proposal must have more Yes votes than No votes, and it must have more than 38,880 Yes votes. A voting ticket would be valid for all proposals during the block that it is used, similarly to how a masternode currently gets 1 vote per proposal.

**Advantages**

This governance strategy fits all goals stated above. It adapts existing systems with comparatively small changes, which avoids complexity that can lead to vulnerabilities. It is easy for a user to understand because once a user understands the reward system, they will already understand most of the voting system. It scales influence according to both investment and participation in the network, and acts as further incentive for people to stake and contribute to the network versus simply holding piv.

Any user on the network with at least 0.1 piv can be included in the staking group and is now included in governance. The interests of both stakers and masternodes are represented without the need for voting layers. Both groups will usually have about 50% of the vote depending on the seesaw algorithm during the cycle, but will also be able to veto or overrule each other with enough votes. Assuming a 50/50 split on ticket distribution for example, an unpopular proposal that is a net -50,000 masternode vote could be overruled if the staking side had a net +50,001 vote to bring the overall approval to 50.1%.

The cost to single-handedly pass proposals or gridlock the system is extremely high in this system compared to other governance models where you may only need to control 51% of one or two layers. It does not require the user to pay a voting fee or lock their funds for any amount of time. It does not encourage centralizing funds in an address which may reduce privacy or distributing funds among many addresses which would add spam to the blockchain. Because there is an effective maximum of 86,398 addresses with rewards during a cycle, the validation strain on masternodes is capped.

This method is as secure as the current PIVX security/reward system and the additional incentives around it would compound on that security. Trying to attack the system only helps the network. Switching between masternodes and staking to seek a higher reward only helps balance the network. To attack the voting system, you would have to invest massively in PIVX and help the network for up to a month collecting voting tickets. Attacks on the MN side would see diminishing returns via the seesaw mechanism diverting rewards to stakers. Attacks on the staking side would be blind since competition is not visible.

**Improvements and comments**

It does not give voting power to non-stakers and non-masternodes like a balance-based system would, but at the time same this method does further incentivize staking with voting rewards. This would therefore exclude users who only utilize mobile or SPV wallets.[1] However, balance-based voting does have some weaknesses like spam/DOS attacks and privacy concerns.

Since voting tickets would be issued right up until the superblock, it doesn’t make sense to force users to vote at the last minute in case they earned another ticket right before the deadline. There are a few ways around this, so the only concern is picking the best one. For example, early voting could be allowed where the user could state their voting intentions at any point during the voting cycle and any future voting tickets before the super block are automatically applied according to the votes they indicated. We could also adjust the ticket collection cycle so it doesn’t align exactly with the superblocks.

Zerocoin compatibility is pending developer review, but I don’t expect issues since staking with zPiv is not possible in the first release.

This proposal is designed as a distribution of voting rights, but does not intend to be the final PIVX governance system. It can be included as a layer of a future system, the approval thresholds can be adjusted, and the proposal structure itself can still be changed. This is meant to be a solid step forward with minimal risk, bringing in the community at large to participate in governance, and get the ball rolling for future improvements.

**Exchange Influence**

The exchange issue is a valid concern and difficult to manage without hindering actual users. Exchanges already could spin up many masternodes and game the current system, but I have not seen any reported cases of this with any masternode or crypto governance system. There seems to be agreement on this topic [in the governance channel](https://pivx.slack.com/archives/C46RT9A9X/p1506369162000451). With that in mind, I’d like to elaborate on this topic in the context of this proposal.

● Staking requires an online computer and exchanges do not want the risk of holding much in a hot wallet. After all the breaches in this space, most will opt for cold storage for the vast majority of their holdings. With this proposal, they would need to stake for some time and this introduces risk that far outweighs the benefit. Additionally, exchanges are high profile targets and would invite far more attacks than your average staker.

● Exchanges are part of the ecosystem and could have some voting weight, just not nearly as much as their holdings

● The fact that PIVX users can get staking rewards means they are less likely to leave as much piv sitting in exchanges, so the exchanges will have less piv in their wallets

● Decentralized exchanges will tie up piv in escrow or smart contracts, not a company’s wallets

Created with direct help and input from:

derek\_hansen @derekcloud

alexanderluthor

a private contributor

Most ideas were sourced from discussions in #governance over the past few months