



PIVX Economics Whitepaper

Version 1.1 - July 2020

Authors: Bryan “SnappySnap” Doreian & Eric Stanek

Contributors: Hank M, CaveSpectre, Strontium, Ambassador

Reviewers: Po’, Liquid369

PIVX.org

© Private Instant Verified Transaction (PIVX) - 2020. All rights reserved



THE FOLLOWING PRESENTATION IS FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS ADVICE, INVESTMENT, LEGAL, OR OTHERWISE.

© Private Instant Verified Transaction (PIVX) - 2020. All rights reserved

Table of Contents

Table of Contents	3
Introduction	4
Helping Decentralized Rights- and Privacy-Preserving Currency	
Succeed by Reducing the Cost And Infrastructure Barriers	5
Economics Specifications	6
Summary:	6
Introduction to the PIVX Network Genesis	7
Initial Parameters	8
The Goal/Purpose of PIV	10
Why Proof of Stake	10
Monetary Policy	11
Coin Emission	12
Reward Distribution	13
Masternodes / Masternode Operators	13
Staking / Stake Node Operators	14
Non-Staking, Non Masternode Operators	14
Economic Forces	14
Lag of Economic Forces	16
Economic Forces Ensure Rewards are Always Fair	16
Masternode Count and Network Strength: Optimum	
Ratios of Stake Nodes to Master Nodes.	17
Maximum Coin Supply	18
Dynamic Coin Supply	18
Tail-End Emission & Inflation	20
Deflation	20
Conclusions	21
Acknowledgements	21



Introduction

Private Instant Verified Transaction (PIVX), launched January 30th, 2016, is a decentralized, open-source, fair-launch blockchain/cryptocurrency project managed, developed, governed, and stewarded by a community driven decentralized autonomous organization (DAO). It is a Proof-of-Stake (PoS) protocol using its custom developed PoS consensus engine with a native cryptocurrency, denominated as “PIV”. PIVX integrates other features including a 2nd layer of functionality through a Masternode network that provides a decentralized governance mechanism of voting; and is currently developing new features for this layer such as the Deterministic Masternode Lists, Long Living Masternode Quorums (LLMQs) and more, as well as including the addition of the anonymity protocol zk-SNARKs Sapling to all transactions and staking—all of these heavily customised. All the PIVX supply occurs as a direct result of a static/fixed block emission rate plus any monthly budget allocation payouts. PIVX also has a dynamically calibrated coin-supply restrained by the burning of transaction fees. PIVX is an independent, application and payment agnostic blockchain. PIVX uses its native cryptocurrency (PIV) as both a means of rights-preserving, privacy enabling, near instant digital currency exchange as well as the reward for those who help secure, build, decentralize, and govern the PIVX network protocol. PIV is purchased and/or obtained to be held or staked (hot or cold) or locked in masternodes by individuals who want to participate in the network.

The monetary policy of PIVX is designed to enable a sustainable infrastructure service capable of supporting scalable, decentralized, and resilient node infrastructure, allowing for instant, private transactions globally, without astronomical Quantitative Easing (QE) and the corresponding resulting devaluation of the native token, as experienced in other cryptocurrency endeavors, especially experienced in many Proof-of-Stake experiments.



Helping Decentralized Rights - and Privacy-Preserving Currency Succeed by Reducing the Cost And Infrastructure Barriers

We believe that rights and freedoms preserving, privacy protecting blockchains like PIVX have the ability to design greater cost efficiencies and reach wider adoption in an efficient, economically sound, and environmentally friendly manner at the protocol layer, while enhancing security and providing resistance to nefarious censorship and or network exploitation of individual rights.

PIVX achieves this through an incentive design that rewards Staking Nodes for collectively securing and decentralizing the network and Masternodes to provide Level 2 network functionality such as instant transactions and governance mechanisms. Further characteristics are:

1. Currency-flow balancing at the protocol level through novel inflationary / deflationary mechanism incentivizes decentralization and minimizes the need for outside monetary policy involvement.
2. Staking with static block reward emission and tail end inflation enables more efficient resource allocation.
3. Low marginal costs for hardware/devices to stake and/or operate masternodes reducing barriers to entry, allowing anyone to participate at any scale, and superior to other projects demanding wasteful energy requirements and hardware needs.
4. Global community run decentralized governance allows for state-less oversight and provides direct community involvement and growth of the project.
5. Advanced Proof of Stake features such as Cold Staking and ancillary technology such as PET4L further enhance the access, security, and freedoms of individuals without burdensome hardware requirements.



Coin Economics Specifications

Summary:

- PIVX has a fixed emission rate per block.
 - 5 PIV as block rewards (2 PIV to Stakers, 3 PIV to Masternodes).
 - 1 PIV allocated (not created) to the budget / treasury.
- PIVX relies on both stakers and masternodes to possess its native token, PIV, to help decentralize, govern, and secure the network.
- Both Masternodes and Stakers earn rewards.
- Equilibrium between the Staking and Masternodes profitability is achieved naturally, as Staking profitability decreases with the increase of the total amount of coins being staked, and Masternode profitability decreases with the increase of the active Masternodes in the network. More detailed explanation is later in the document.
- Users of PIV pay a small transaction fee per transaction.
- All transaction fees are burned, removing coins from the total supply.
- PIVX has a tail emission. (A tail emission is important because the block rewards are incentives for network participants to continue hosting and securing a healthy network without passing costs on to users in the form of high fees.)
- Annual PIVX inflation rate is currently around 5%, with the slow and steady decrease over time as emission rate per block stays fixed. Thus, the inflation rate decays towards 0% through time organically.
- Transaction fee burning acts as an economic thermostat - as transactions increase, so does the corresponding coin burning.



Introduction to the PIVX Network Genesis

Private Instant Verified Transaction (PIVX) was announced on bitcointalk.org on November 25th, 2015. For historical purposes, PIVX was originally launched under the name Darknet (DNET) and officially rebranded to PIVX on January 1st, 2017. On January 30th, 2016 it was announced that PIVX (DNET) would officially be released and at 04:10:07 UTC on January 30th, 2016, the first block of the PIVX network was created.

In its PoW phase in order to launch the network, PIVX utilised the Quark algorithm as it was deemed most fair due to its less exclusive technical limitations. After a period of 259200 blocks, Proof of Work was stopped and replaced with Proof of Stake in order to provide a more robust, lower economic barrier, more energy efficient and long term sustainable means of securing the network and rewarding those participants who help secure and govern the network. Thus, expensive, hardware limiting mining was replaced with energy efficient, simpler to operate stake node operators. A 2nd layer to the blockchain was carried forward as well, this layer often being referred to as a Masternode layer. This layer provided the governance mechanisms as well as instant transaction capabilities.

The PoS model was initially designed and implemented to incentivize masternode operators over stake node operators to ensure a robust layer 2 network, until a certain critical mass of masternodes was achieved for a stable and robust network. This critical mass target was designed for when the number of masternodes and number of stakers resulted in a 50:50 split of the block reward. This equilibrium under the initial reward payout parameters would have required 35-40% of the total coin supply (roughly 20-30million PIV by today's numbers). When the implementation of the zerocoin protocol and zPIV staking was introduced, in order to preserve the integrity of the privacy pool the block reward payout structure had to be altered to fixed integers, and with this, changed from a dynamic payout to a fixed integer reward payout. When the Zerocoin protocol was deprecated, the reward was further updated to its current status of 3 PIV per block to MN operators, 2 PIV per block to stakers, and up to 1 PIV per block allocated for proposals requesting budget payouts. More on this element below.

It should be noted that if the network was currently running the original block reward structuring, 1.75 PIV would be going to stakers, and the MN would be receiving 3.25 PIV. (June 18th, 2020 - 1617 total Masternodes)



Initial Parameters

PoW Phase Period: January 31th 2016 to August 17th 2016 (FINISHED)

Proof of Work phase rewards breakdown

Block height	Masternodes	Miner	Budget
1*	**	**	**
2-86400	1/3 (83 1/3 PIV)**	2/3 (166 2/3 PIV)	***
86401-151200	20% (50 PIV)	70% (175 PIV)	10% (25 PIV)
151201-259200	45% (22.5 PIV)	45% (22.5 PIV)	10% (5 PIV)

* 60001 PIV were premined on the genesis block for the purpose of setting up 6 initial Masternodes. This premine was burnt on block 279917. There was no instamine.

** Masternodes were paid when available for a period of time, before payment was enforced.

*** Proposal successfully voted by MN holders at that time to allocate 1 million DNET from the budget/treasury superblock to go to a general fund (April 3rd, 2016) - the first ever budget payout of the DNET/PIVX ecosystem.



PoS Phase Period: August 17th 2016 onward starting at block 259201 (CURRENT)

Proof of Stake phase rewards breakdown

Phase	Block height	Reward	Masternodes & Stakers	Budget
Phase 0	259201-302399	50 PIV	90% (45 PIV)	10% (5 PIV)
Phase 1	302400-345599	45 PIV	90% (40.5 PIV)	10% (4.5 PIV)
Phase 2	345600-388799	40 PIV	90% (36 PIV)	10% (4 PIV)
Phase 3	388800-431999	35 PIV	90% (31.5 PIV)	10% (3.5 PIV)
Phase 4	432000-475199	30 PIV	90% (27 PIV)	10% (3 PIV)
Phase 5	475200-518399	25 PIV	90% (22.5 PIV)	10% (2.5 PIV)
Phase 6	518400-561599	20 PIV	90% (18 PIV)	10% (2 PIV)
Phase 7	561600-604799	15 PIV	90% (13.5 PIV)	10% (1.5 PIV)
Phase 8	604800-647999	10 PIV	90% (9 PIV)	10% (1 PIV)
Phase 9	648000-1154203	5 PIV	90% (4.5 PIV)	10% (0.5 PIV)
Phase 10	1154203-1686229	6 PIV	83.3% (5 PIV/zPIV)	16.6% (1 PIV)
Phase 11	1686229-Current	6 PIV	83.33% (5 PIV)	16.6% (1 PIV)



The Goal/Purpose of PIV

PIVX is a transactional freedom and privacy preserving cryptocurrency. The PIVX blockchain is engineered to have sub 1-second transactions, allow for network scalability to accommodate thousands of transactions per second, facilitate direct P2P payments, all while:

1. Providing privacy preserving features and mechanisms to ensure individual rights are maintained.
2. Providing inclusiveness of the PIVX blockchain/cryptocurrency to anyone, by lowering the barrier for energy, hardware, and technological barriers common to many other cryptocurrency projects.
3. Providing a sound, robust economic model for long term fiscal sustainability that rewards network participation fairly, and encourages use and adoption of new network participants.

Why Proof of Stake

The PIVX network functions on a Proof of Stake consensus algorithm, which was introduced in a paper by Sunny King and Scott Nadal in 2012¹. The original concept relied heavily on the notion of “coin age”, or how long a UTXO (Unspent Transaction Output) has not been spent on the blockchain. In this way, it differs from Proof of Work by not focusing on and rewarding miners, but rather rewarding anyone willing to participate in the running of the network. The protocol was further refined in PoS version 2 for BlackCoin by Pavel Vasin (Rat4) with several potential security fixes, such as the potential of a malicious node to abuse coin age to perform a double spend; or the potential for honest nodes to abuse the system by staking only periodically, negating coin age from consensus². The robustness and innovation of PIVX’s Proof-Of-Stake was further enhanced in an updated of the protocol at the end of 2016³, then with the novel implementation of Zerocoin Proof of Stake (zPoS) by PIVX in 2018⁴, and through 2019-2020 has undergone further improvements and security updates, for example the new Time Protocol. In this way, PIVX has pioneered forward the original concepts of Proof of Stake, with its continual development providing superior security as well as the novelty of a corresponding masternode layer and privacy features.

¹ S. King, S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.

² P. Vasin, BlackCoin’s Proof-of-Stake Protocol v2, <https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>

³ BlackCoin, Security Analysis of Proof-of-Stake Protocol v3.0, <https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf>

⁴ <https://pivx.org/zpiv/>



Simply put, staking is making computing resources available to the network, which may “select” the node to generate the upcoming block on the chain based on delimited competition. In the case of PIVX, these limits are demarcated by considering the balance (UTXOs) staked by the wallet—every staking node is competing trying to create a valid block, very much like in PoW. Nodes, however, are technically limited in the number of trials in a given time (eliminating the need for higher computing power) and the difficulty to get a valid block is inversely proportional to the amount being staked. A higher balance means a higher chance of satisfying the difficulty criteria, validating the block, and being rewarded. Staking is significantly less demanding on resources than PoW mining, as there is no need to push towards ever increasing difficulty, and the associated increase in computing power to solve it. As such, PoS is an environmentally friendly alternative to PoW.

While the environmental factor alone already helps PoS stand out against PoW, there is another factor to be considered: maintaining a fair, distributed power across the network, which should be a high priority target of any cryptocurrency. With the expanding difficulty in mining that necessitates more powerful rigs that cost more to run, the ability for people to feasibly operate such rigs becomes more exclusive. Such things as the costs of hardware, electricity consumption spent on computing, and further consumption on cooling, rule out a great many locations as suitable for mining. Inevitably, this results in a great deal of power held by miners, of which fewer and fewer are able to remain competitive, not only leading to a monopoly in rewards, but in control over networks. As such, Proof of Stake and thus PIVX present a far lower economic and resource dependent barrier to adoption and use globally. Lastly, setting up a mining rig requires way more technical knowledge than setting up a staking node, which opens up a space for wider adoption and involvement of non-technical users.

Monetary Policy

PIVX’s monetary policy will be dictated by how its primary economic levers are influenced and adjusted over time with the mandate to ensure long term stability, sustainability, and accessibility of the protocol. The monetary policy is governed directly by the blockchain codebase, indirectly governed by the use of the network by users (as burnt transaction fees play a role in the deflationary lifecycle aspect of the monetary policy), and indirectly able to be controlled by the PIVX DAO and its participants by way of protocol level governance anonymous voting.



The primary economic levers managed by the monetary policy are (but not limited to):

1. Transaction Fee Cost and Burn.
2. Rate of coin emission per block.
3. Split of coin emission rewards per block between stakenodes and masternodes.
4. Minimum amount for staking.
5. Requirements for Masternode.

Coin Emission

PIVX creates a new block every 60 seconds. Each of these blocks create 5 new PIV, and allocates 1 new PIV. What does 'allocate' mean? To understand that, the PIVX governance model needs to be understood.

The PIVX governance model is a system that allows for funding to be generated for community proposals. Proposals are submitted to the system by the community, and they are voted on once a month. Those proposals that "pass" are issued the funds they have requested. This fund issuance occurs in a "Super Block", which occurs every 30 days. The available funds for each Super Block equals the number of blocks since the last Super Block, times the number of PIV allocated for the Super Block from each block. The math here is fairly simple, especially since this is where the one 'allocated' PIV comes into play. One PIV per block, and one block every minute, for 24 hours for 30 days works out to be $30 \text{ days} \times 24 \text{ hours a day} \times 60 \text{ minutes per hour} \times 1 \text{ PIV per block} = 43,200$ PIV allocated to the Treasury per Super Block. This forms the "budget" available for the proposals.

When the Super Block is created each month, the Masternodes reach a consensus on the proposals that have met the required number of yes votes. To be considered for funding, the difference between the yes votes and no votes must be greater than 10% of the number of Masternodes on the network. For example, if there are 1,500 Masternodes, a proposal must have 150 (10% of 1,500) more Yes votes than No votes.

The proposals are sorted by their "net yes" votes (yes votes minus no votes) and they are then paid in order from highest "net yes" to lowest.

The total PIV required to fund all the passing proposals is rarely identical to the 43,200 budget. If the total funds needed for all passing proposals is "under budget", not all 43,200 are created. For example, if all passing proposals total 40,000 PIV, then only 40,000 PIV are created and paid to those proposals. This does not mean that the full budget of 43,200 PIV was created, and the unspent 3,200 PIV are burned or held for the next Super Block. This



is what is meant by 'allocated'; 1 PIV is allocated from each of the 43,200 blocks between Super Blocks to form the budget, but only enough to fund the proposals is actually created when the Super Block is created. In the example scenario, the extra 3,200 PIV are not created in the first place. Only the 40,000 PIV needed are created.

Conversely, if the passing proposals exceed the 43,200 PIV budget, proposals are paid out in order until there is not enough room in the budget to pay any of the further proposals. For example, if there are 4 passing proposals asking for 10,000 PIV each, (40,000 total) and all the remaining passing proposals ask for more than 3,200 PIV, then none of the remaining proposals will be paid, and only the first 4 will be paid. In this scenario, again only 40,000 PIV are created.

It is possible that exactly 43,200 PIV can fund passing proposals, with nothing remaining. But, this is rare.

Most of the time, a very high percentage (Usually 95% or more) of the allocated 43,200 PIV is created to fund proposals. As such, it is reasonable to estimate inflation to be based on 6 PIV per block being created. However, it is important to realize this is not exact. It is also important to realize that the PIV for Treasury funds is created at the Super Block, whereas the other 5 PIV is created with each standard block.

Reward Distribution

- 2 PIV per block is created and paid to the staker that wrote the block.
- 3 PIV per block is created and paid to the next masternode in the payment queue.
- 1 PIV per block is allocated to the Treasury Budget and [may be] created with the Super Block and paid to a funded proposal.

Masternodes / Masternode Operators

Masternodes are a 2nd layer of functionality for the network. They determine Governance Voting consensus for Proposals. They also add some stability to the amount of coins available for purchase on the market. Setting up a Masternode does involve some effort, and while a Masternode owner can unlock those coins to Staking instantly, relocking them, or allocating them back to a Masternode takes effort, and several days of waiting to get back into the top of the payment queue. As such, Masternode Owners tend to just HODL.



There are multiple ideas being discussed, for future functionality for Masternodes, such as the Deterministic Masternode Lists, Long Living Masternode Quorums (LLMQs) and more. Therefore, it is expected that over time, Masternodes will serve an even more significant role in the greater PIVX ecosystem.

Staking / Stake Node Operators

Stakers secure the network and build the blockchain by creating the blocks and submitting them to the network.

Non-Staking, Non Masternode Operators

There are some wallets that do not Stake, or have collateral for a Masternode. These are typically exchanges or people with less than 10,000 PIV for a Masternode, or that can't keep their computer on 24x7x365. Cold staking helps with the latter, and some exchanges now provide Staking services for PIV deposited with them; but regardless, there is a significant amount of PIV that is not Staking or in a Masternode.

Economic Forces

The PIVX Economic Model assumes that people will make decisions that maximize their ability to earn rewards.

At first glance, this makes it look like everyone would move their PIV to a Masternode, to earn 3 PIV per block, instead of Staking and only receiving 2 PIV per block. However, it is a little bit more complex than that.

Let's start with 2 rooms, a 'Staker Room' and a 'Masternode Room', each with 25 people. Now, let's assume that people are free to move from room to room. Granted, this is not true in the real world, as you need 10,000 PIV to be a Masternode Owner and some of the Stakers will not have that many PIV. However, in the real world, the above 'closed system' does not exist and there is always someone in the crypto space with enough wealth to own 10,000 PIV to invest in PIVX. As such for the purpose of this explanation, it is perfectly acceptable to assume free movement from one room to another. To make things simple, we can also assume that each person has 10,000 PIV. This also is not true in real life, but the math below is on a 'per person per PIV' basis, so it is moot.



If the PIVX network pays 2.5 PIV per block to the Staker Room, to be evenly distributed among Stakers, and 2.5 PIV per block to the Masternode Room, to be evenly distributed among Masternode Owners, then they each are making the same rewards, and due to Economic Forces, no one moves from one room to another. We have the following:

Scenario 1: Staker and Masternode Rewards are the same. Balanced.

	Staker Room	Masternode Room
People:	25	25
Rewards per block:	2.5	2.5
Profit Per Person Per 25 mins:	2.5	2.5

Now let's change the rewards to what they currently are for PIVX. Then we have the following:

Scenario 2: Staker rewards are less than the Masternode rewards. Not balanced.

	Staker Room	Masternode Room
People:	25	25
Rewards per block:	2.0	3.0
Profit Per Person Per 25 mins:	2.0	3.0

Clearly, in this scenario, it is more profitable for people to be in the Masternode Room. So, as they see this opportunity, they move to that room. Eventually, the Economic Forces balance out, and the profit is the same for each person again and we have the following:

Scenario 3: Staker rewards are less than the Masternode rewards. Balanced.

	Staker Room	Masternode Room
People:	20	30
Rewards per block:	2.0	3.0
Profit Per Person Per 25 mins:	2.5	2.5

Similarly, Economic Forces would also create the following scenario:

Scenario 4: Staker rewards are greater than the Masternode rewards. Balanced.

	Staker Room	Masternode Room
People:	30	20
Rewards per block:	3.0	2.0
Profit Per Person Per 25 mins:	2.5	2.5



Lag of Economic Forces

Currently, the ratio of PIV Staking to that in Masternodes is not balanced, and rewards are higher for Masternodes. There are 3 reasons for this.

First, it is easier for Masternode operators to move PIV to Staking than it is for Stakers to move PIV to Masternodes. This is due to:

- 1) the extra effort required to setup a Masternode.
- 2) the loss of income for the several days for a Masternode to get to the top of the queue. This variable will likely remain and simply cause a 'dampening' effect in moving to the balance point.

Second, not everyone has 10,000 PIV, and therefore additional Masternode Owners often come from outside the PIVX ecosystem to invest. This is good though, because it drives up the demand of PIV and therefore the price. This also causes a 'dampening effect' albeit one that should disappear over time as PIVX becomes more well known.

Third, operating a Masternode often incurs a cost for a VPS. This is changing though; as distribution increases and more and more people run their own at home, sometimes on SBCs such as the Raspberry Pi. Likewise as the value of PIVs rise, the overhead cost, as a percentage of their monthly rewards, drops. As such this reason should disappear over time.

Economic Forces Ensure Rewards are Always Fair

Given the above scenarios, and the fact that regardless of reasons for a balance of rewards between Masternodes and Stakers to lag, the key fact is that they do bias to being fair and equal. As such, the only thing that is achieved from changing the reward distribution between Stakers and Masternodes, is the number of Masternodes, and the amount of PIV securing the network.



Masternode Count and Network Strength: Optimum Ratio of Stake Nodes to Master Nodes.

Is the current reward distribution of 3 PIV per block to Masternodes, and 2 PIV per block to Stakers optimized? Answering that question is beyond the scope of this document. But, if after extensive research and analysis (keeping future Masternode functionality in mind) it makes sense to change the number of Masternodes and the amount of PIVX being Staked, then the PIVX Core Development team will likely make changes to the protocol. Both Stakers and Masternode Owners will be fine with it, because Economic Forces will create a new balance point, and rewards will again be fair.

Scenario 1: 40M PIVX shared between stake operators and masternode operators.

What's best (for the network)?

20M staked and 2000 masternodes?

24M staked and 1600 masternodes?

32M staked and 800 masternodes?

Currently, the tradeoffs include a myriad of variables. With more individuals staking, in theory there is more active network security/stability. However, while the total emitted reward per block going to those stakers remains fixed (2 PIV per block), the net rewards each stake node operator experiences may in fact decrease as more stake operators stake, simply due to more nodes participating in the network and thus receiving stake rewards. With this and presumably less masternodes, that 2nd layer of functionality (currently the governance voting mechanism and budget authorization protocol) is not as robust. Less masternodes results in less potential voting. Also as new functionality is being programmed for this 2nd layer, less masternodes equals a less robust layer. While the total emitted reward per block going to those masternodes remains fixed at 3 PIV per block, each of those masternode operators may actually experience an increase in payout frequency (less MN nodes = your MN node will cycle through the payout queue faster).

As there are multiple aspects involved (and some of them are in the process of being changed), this is not an easy question to answer as to just "what" is the optimum ratio between stake nodes and masternodes.

With the current static block reward/emission rate of:

2 PIV to Stake node

3 PIV to MasterNode

There is enough incentive currently to those desiring a masternode to run one (paying for



hardware/infrastructure costs), but not so much as to make running one disproportionately more economically favorable than staking. As we will talk about below, staking offers a much broader element of inclusiveness, as the economic barrier for staking is limited to essentially only requiring 1 single PIV.

Since proof-of-stake was first introduced back on July 31, 2016 the reward split was, by design, a sliding scale with the intention of incentivizing MNs until a threshold of critical mass was achieved (which it never achieved).

The code as it was written then outlined that the situation where the reward split was 50:50 would have been if the number of coins held in MNs was between 35-40% of the total coin supply. To this day, that amount has never been achieved in the history of the chain.

If PIVX were still running with that prior code now (reward of 5 PIV between MNs and stakers), the staker would receive 1.75 PIV, and the MN would receive 3.25 PIV.

Thus, PIVX has shifted it's economic reward scale slightly from incentivizing masternode operators to stake node operators with it's 3 PIV to MN, 2 PIV to staker block reward distribution.

Maximum Coin Supply

The numbers below represent the theoretical maximum coin supply. The actual number will be determinant upon transaction fee burning and allocated PIV not required, of the maximum possible monthly budget generation. As a result of these factors, the actual number will most likely be less than these theoretical maximums.

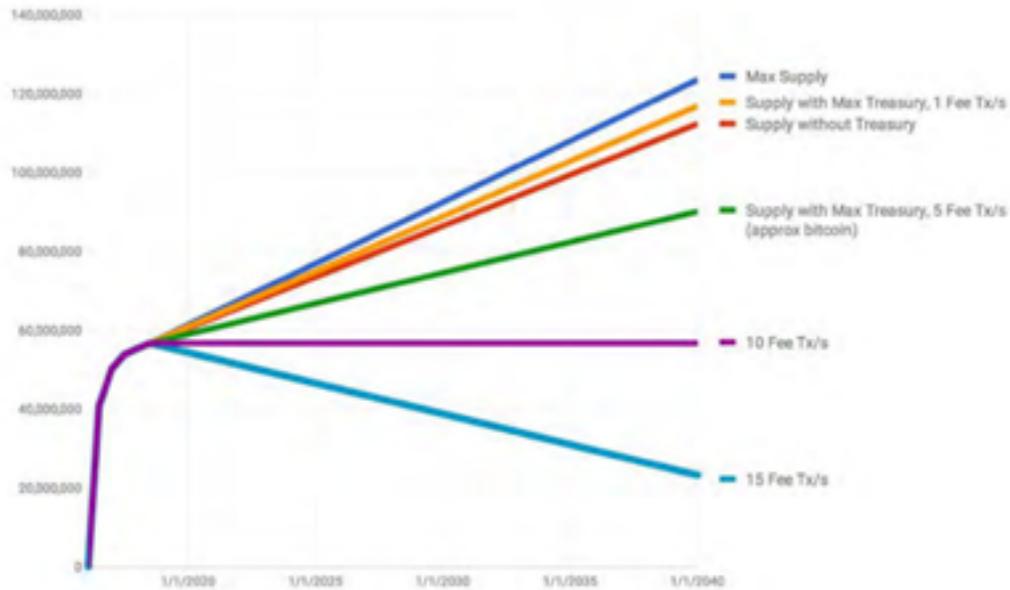
By June 2020: 62,857,497 PIV

By June 2040: 125,929,497 PIV

By June 2060: 189,001,497 PIV

Dynamic Coin Supply

Although PIVX features no hard cap on its coin supply (a defined absolute limit), it does have a soft cap (a restriction on the number of coins produced when a certain condition is met). The PIVX soft cap condition is met when fees charged on network actions amount to that minted within a block. The blockchain will then start burning the same amount of coins as it is generating, limiting growth. Thus, PIVX features a dynamic coin supply calibrated by the blockchain in reaction to action of the network.



In this image, you can see the soft cap conditions in an approximate model. It shows what would be the max coin supply should each monthly budget be 100% utilised, and what the new soft cap would look like at different meaningful (non-standard) transaction volumes (as to trigger significant fee burns). When fee burns outpace the 6 PIV generated per block as block rewards, the graph trends down, rather than up.

To explain in more detail, the dynamic coin supply of PIVX has a similar philosophy to that of an elastic currency⁵⁻⁶, where the money supply is adjusted in response to economic pressures— i.e. business volume—to target stability. This is achieved by calibrating circulating volume to credit volume. Elasticity in a money economy is executed by withdrawing currency from circulation. This occurs upon a decision in response to a turning market. This action nudges the economy in the desired direction.

Unlike elastic currency, however, PIVX does not contract upon an executive decision to do so, nor does it react to calibrate circulating volume to credit volume. The only influencing factors are those based upon transaction volume and fee burning as interpreted by an algorithm. At a high rate of transactions per second, the coin supply burning will equal the same amount as it is generating, creating a neutralising effect on the coin supply. This soft cap value is not a simple number to predict, however, as fees vary. For example, compared to standard PIVX transactions, SwiftX transactions have higher fees. There also exist options

⁵ <https://archive.org/details/encyclopediaofba00woel/mode/2up?q=elastic+currency>

⁶ http://www.eagletraders.com/advice/securities/elastic_currency.php



within the PIVX Core wallet to opt for custom fees, with the ability to set them higher than default. These variables make giving a flat transaction rate per block on the neutralising effect impossible.

It's important to note that the emission-vs-burn balancing algorithm controls the coin supply in response to the most recent state of the blockchain. No developer, owner, miners, or any other party can create new coin supply. The algorithm ensures that the lack of a coin-supply hard cap works in favour of a healthy economy for PIVX as a currency. Since the block time target is 60 seconds with PIVX, the economy is maintained by the minute, daily.

In the event the balance of the PIV burning algorithm becomes unfavourable for the health of the PIVX economy, the issue can be taken up by the decentralised government to vote upon the best solution.

Tail-End Emission & Inflation

Inflation in money/fiat currencies is often seen in a negative light. It impacts on the purchasing power of a currency, reducing the value of a unit of currency over time. Inflation stems from a growing supply of money, which is where it has its roots. When gold and silver were traded, the more of each was brought into an economy, the less rare it became, and so it lost some purchasing power. Gold and silver could also be debased by mixing cheaper metals in when minting new coins, increasing coin supply at the cost of fungibility. Most currencies now, however, are fiat, and not backed by gold or silver. Despite this, inflation remains. Inflation exists today as a mechanism to accommodate a larger user base of an economy's currency participating in more markets. It also serves to counteract excessive value of interest gains - if one far exceeds the other, the economy quickly becomes unhealthy. The counterpart of inflation is deflation - an instance of the buying power of a currency increasing. Both inflation and deflation are matters of supply and demand within a currency.

Deflation

Deflation, when based on user-base can be demonstrated with a simplified example. If 100 coins exist between a user-base of 100 people, each coin's value is rather moderate. If 900 more people were to begin participating in the economy, the rarity of the coins per-head would greatly increase their value. With the PIVX network emitting PIV with each new block, inflation may initially seem a concern. It's important to note, however, that the PIVX economy is very different from those based on money or fiat currency. Unlike gold or silver coins, PIV are divisible, and cannot be debased, so they maintain fungibility. Unlike fiat currencies, PIV are not tied to any national debt, and are always credit-neutral. Lastly, newly minted PIV are distributed to the community freely, so



any loss of purchasing power PIV might experience as the supply increases (which happens only gradually due to fee burning) is offset by the ‘interest’ accrued by staking rewards, masternode rewards, and budget spending.

Conclusions

There are still many barriers to widespread cryptocurrency adoption and use. Further still, there are few projects that provide both a low economic, technical, and hardware requirement barrier while also providing full freedom of privacy maintaining protocols. As a result, the majority of the crypto ecosystem is currently onboarding only more “technologically” and “resource heavy” regions, and to their own detriment of giving up freedoms, rights to privacy, and in some cases, long view economic sustainability. This document outlines the economic primitives used to incentivize a sustainable infrastructure service capable of supporting scalable, decentralized, and resilient node infrastructure, allowing for instant, private transactions globally with PIVX.

Acknowledgements

This economic model paper comes from countless conversations, economic theory research and efforts of others. Firstly, thanks to the originators of the PIVX network and early miners for helping to launch the network. Thanks to the current development team that is pioneering Proof of Stake and turning this model into a global reality. Thanks for the stakers and masternode owners, for helping to secure the network. Thanks to Strontium for your work in 2018 compiling a lot of data that was incorporated here. Thank you to Cave Spectre, Hank M, Jakiman, Ambassador, and Terrik for your insights and collaborative conversations.