PIVX: Protected Instant Verified Transaction

[whitepaper version 2.0 (non-technical)]

Bryan W. Doreian (Snappy) Ryan R. Erickson (ConsistentNot)

ABSTRACT

An engaged, robust, active community with the means for adequate governance and decision-making processes is fundamental to the success of any decentralized, peer-to-peer cryptocurrency. The protection of personal information, especially financial data, is essential to preserve everyone's rights. It is not practical, nor historically wise[1], to trust centralized regulatory entities to protect an individuals' data appropriately. Additionally, without a proper system of governance, it is equally unwise to trust a cryptocurrency project or a specific blockchain with claims of being decentralized, as a single individual can hijack the network, unilaterally make a decision, or worse, lose access rending the codebase unaccessible. (See the decentralization of PIVX here[2].)

Furthermore, for an emerging cryptocurrency project to thrive in a world where:

a. Energy is not taken for granted,
b. It has a solid economic model for growth without massive Quantitative Easing devaluation through inflation, and
c. It allows access to participate and earn from the global network from any low power device (e.g., mobile phone),

There must be a conscious thought into the algorithm selected (proof of work vs. proof of stake), the underlying economic system, and a means of network participation.

This is where the **P**rotected **I**nstant **V**erified Transaction (**X**) (PIVX) project comes in. The preservation of your rights and freedom, secured financial data, and privacy-protecting blockchain, can leverage greater cost efficiencies and reach wider adoption in an efficient, economically sound, and environmentally friendly manner at the protocol layer. The project does this while enhancing security and providing resistance to nefarious censorship or network exploitation of individual rights.

To solve these problems and gaps in the current cryptocurrency landscape, PIVX incentives every node in the network to be part of the block generation process through the implementation of a Proof of Stake consensus algorithm to decide which block will be chained next. Another layer to the network contains Masternodes, that provide Level 2 networking functionalities such as governance mechanisms. Further characteristics are:

1. Currency-flow balancing at the protocol level through novel inflationary/deflationary mechanisms incentivises decentralization and minimizes 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.

[1] https://www.investopedia.com/articles/investing/011916/brief-history-us-banking-regulation.asp
[2] https://www.coinexplorer.net/PIV/network/geo-location

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 (PIVX's Emergency Tool For Ledger) further enhancing individuals' access, security, and freedoms without burdensome hardware requirements.

The entire PIVX ecosystem is akin to being a decentralized, self-organizing, virtual private on-demand network (VPN), but for money.

1. INTRODUCTION

The advent of the blockchain era occurred in 2009 via the creation of *Bitcoin* and its underlying technology by the entity known as Satoshi Nakamoto. Following Bitcoin's success, many competing cryptocurrencies—often referred to as alt-coins—have launched. Bitcoin's launch, and original whitepaper, built upon a 1991 concept[3] to create the digital ledger system that many recognize as today's blockchain. The blockchain's potential to revolutionize digital transactions and how business is conducted worldwide has seen an explosion of interest in the technology.

Currently, the market is awash with tokens and coins from parties of varying intent, motivation, and affiliation. Though there are a myriad of projects, some novel and ambitious, many others are in essence clones with catchy names, and have served as a deterrent to much broader adoption of cryptocurrency as a legitimate and borderless alternative to fiat currency. Bitcoin, despite its innovations, has failed to be widely accepted and adopted as a currency and remains widely viewed as a store of value rather than means of conducting everyday business. The project has further suffered a backlash on its excessive use of electricity needed for maintaining its network and mining its coins.

With over a decade since Bitcoin's launch, a definitive identity for cryptocurrencies has yet to emerge. The overall ambiguity has caused the public to view the crypto-marketplace as a stock market 2.0 and not a means of currency. An inherent volatility and saturation intimidate potential adopters, who regard it not as an alternative to fiat currencies but as a risky investment opportunity.

In keeping with the spirit of cryptocurrency's defining goal, PIVX aims to bring together the tech-savvy and tech-wary. It strives to provide a safe means through which investors and the general public can conduct business without the need for financial institutions or middle-men. PIVX provides the people of an ever more interconnected world with a practical and protected means to conduct business on one's behalf.

[3] https://www.investopedia.com/terms/b/blockchain.asp

“The main point of cryptocurrency is to fix the problems of traditional currencies by putting the power and responsibility in the currency holders’ hands. All of the cryptocurrencies adhere to the 5 properties and 3 functions of money. They each also attempt to solve one or more real-world problems.”
~ Mike Chu, DataOverhaulers.com

2. NETWORK DESIGN

2.1 Introduction to the PIVX Network Genesis

Protected Instant Verified Transaction (PIVX) was announced on bitcointalk.org on November 25th, 2015[4]. 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[5] it was announced that PIVX (DNET) would officially be released and at 04:10:07 UTC on January 30th, 2016[6], the first block of the PIVX network was created.

Today, PIVX, as it was when first launched, is decentralized, incentivised, and open-source.

The project originally launched using the Proof of Work[7] (PoW) consensus model in order to fairly launch the network. PIVX implemented the Quark hashing algorithm[8] as it was deemed most fair due to its less exclusive technical limitations. The network started with 60-thousand PIV (The coin of PIVX) being premined on the genesis block[9] for the purpose of setting up six initial Masternodes. However, this premine was burnt on block 279917. There was no instamine, and no PIV were locked away in order to manipulate the PIVX economy. After a period of 259200 blocks, PoW was replaced with Proof of Stake[10] (PoS) consensus model in order to provide a more robust, lower economic barrier, energy efficient, and long term sustainable means of securing the network. All while rewarding those participants who help secure and govern the network. Thus, expensive hardware limiting mining was replaced with energy efficient, simpler to operate, stake nodes. A 2nd layer to the blockchain was carried forward as well, this layer often being referred to as a Tier Two Network layer. This currently provides the governance mechanisms, and will shortly provide an entire new array of features for the Network.

[4] https://bitcointalk.org/index.php?topic=1262920.0
[5] https://bitcointalk.org/index.php?topic=1262920.40
[6] https://explorer.pivx.link/block/000005504fa4a6766e854b2a2c3f21cd276fd7305b84f416241fd4431acbd12d
[7] https://www.investopedia.com/terms/p/proof-work.asp
[8] https://cryptorival.com/algorithms/quark/
[9] https://www.investopedia.com/terms/g/genesis-block.asp
[10] https://www.investopedia.com/terms/p/proof-stake-pos.asp

PoW Phase Period: January 31th 2016 to May 21st 2016 (FINISHED)

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.*

*** 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: May 21st 2016 onward starting at block 259201 (CURRENT)

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	1154204-1686229	6 PIV	83.3% (5 PIV/zPIV)	16.6% (1 PIV)
Phase 11	1686230-Current	5 PIV	83.33% (5 PIV)	16.6% (1 PIV)

2.2 Proof of Stake

The PIVX network currently operates on a PoS consensus algorithm, which was introduced in a paper by Sunny King and Scott Nadal in 2012[11]. The original concept relied heavily on the notion of "coin age," or how long a UTXO (Unspent Transaction Output[12]) has not been spent on the blockchain. In this way, it differs from PoW by not focusing on and rewarding miners, but rather rewarding anyone willing to participate in the running of the network (holding their coins on a node). The protocol was further refined in PoS version-two for BlackCoin by Pavel Vasin (Rat4) with several potential security fixes. Vasin's fixes included the potential of a malicious node to abuse coin age to perform a double spend, the potential for honest nodes to abuse the system by staking only periodically, and negating coin age from consensus[13]. The robustness and innovation of PIVX's PoS model was further enhanced in an update of the protocol at the end of 2016[14] with the novel implementation of Zerocoin Proof of Stake (zPoS) in 2018[15]. Since then the project has undergone further improvements and security updates, for example, the new Time Protocol[16]. PIVX has pioneered beyond the original concepts of PoS with its continual development providing superior security and the novelty of a corresponding Masternode layer and financial data protection features.

Through the implementation of PoS, the network has computing resources available which automatically 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 to create a valid block, very much like 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 (i.e., Bitcoin), as there is no need to push towards ever increasing difficulty to solve algorithms necessary to mint coins, and the associated increase in computing power to solve said algorithms. 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 distribution of power across the network, which should be a high priority target of any cryptocurrency. With the expanding difficulty of PoW mining that necessitates more powerful devices (aka rigs) that cost more to run, the ability for people to feasibly operate such devices becomes more exclusive. Real life barriers to the average person in PoW operations include costs of hardware, electricity consumption spent on computing, and further consumption on cooling. Inevitably, this results in a great deal of power held by smaller groups of miners, of which even fewer will be able to remain competitive, not only leading to a monopoly in rewards, but in control over networks. PIVX's use of PoS over PoW presents a far lower economic and resource dependent barrier for adoption and global use. Furthermore, setting up a PoW mining device requires more technical/advanced knowledge than

[11] S. King, S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.
[12] https://www.investopedia.com/terms/u/utxo.asp
[13] P. Vasin, BlackCoin's Proof-of-Stake Protocol v2, https://blackcoin.co/blackcoin-pos-protocol-v2- whitepaper.pdf
[14] BlackCoin, Security Analysis of Proof-of-Stake Protocol v3.0,
https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf
[15] https://pivx.org/zpiv/
[16] https://github.com/PIVX-Project/PIVX/pull/1002

setting up a staking node, which opens up a space for wider adoption and involvement of non-technical users.

2.3 Masternodes

The PIVX network is two-tiered. The staking tier is the first, in which all PIVX holders can participate through staking their PIV; the second is the Masternode tier. Masternodes are a set of incentivised nodes within the PIVX network responsible for the handling of particular specialised tasks. The PIVX Masternode network has its roots from the cryptocurrency Dash, with a significant restructuring to a Proof of Stake consensus algorithm. As such, these nodes are an integral part of the PIVX digital ecosystem, and necessary to network functionality.

The Masternode network fulfils a range of functions independent of staking nodes. These distinct functions are limited to Masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no single Masternode has power or authority in excess of others on the network.

2.3.1 Deterministic Masternodes

Deterministic Masternode lists are lists of Masternodes, built at every block, relying only on on-chain data (previous list, and transactions included in the current block).

All nodes derive (and verify) their Masternode lists independently, from the same on-chain transactions, thus they immediately reach consensus on the tier-two state (number of Masternodes, properties and status of each one).

As clearly explained in the "motivation" part of the DIP document[17], this is crucially different from the previous system:

> *"The previous system was maintained with consensus mechanisms that predated Satoshi Nakamoto's solution to the Byzantine Generals Problem. This meant that each node needed to maintain their own individual Masternode list with P2P messages and not a blockchain based solution. Due to the nature of the P2P system, there was no guarantee that nodes would come to the same conclusion on what the Masternode list ought to look like. Discrepancies might, for example, occur due to a different order of message reception or if messages had not been received at all. This posed some risks in regard to consensus and limited the possible uses of quorums by the system.*
>
> *As a concrete example, the previous system required implementing workarounds such as "Masternode reward voting" which was performed multiple blocks in advance for each block to make sure that consensus would be found and agreed on. Enforcing this consensus however still posed a risk which could have resulted in network wide forking, so a spork to turn off Masternode*

[17] https://github.com/dashpay/dips/blob/master/dip-0003.md

payment enforcement was added to prevent this issue from occurring. The spork was used sporadically after major network updates."

This is a major overhaul, which brings also a good number of improvements in the user experience, while removing the shortcomings of the previous system.

For a deeper analysis of Deterministic Masternodes, please review the DIP3[18] document, which describes perfectly the advantages of the new system.

2.3.2 Masternode Roles

For each Masternode, three different "roles" are defined. Each role is represented by a private/public keypair.

1. Owner: Must be unique on the network. Can update the other two roles, and the Masternode payout address.
2. Operator: Must be unique on the network. The operator key is saved in the pivx.conf of the remote node, and it is used to sign Masternode-related P2P messages (e.g. budget finalizations, or Masternode winners in the compatibility code). It can also be used to update the Masternode IP-address, or the operator payout address (if the Masternode is configured to allow a percentage of the reward to be paid to the operator).
3. Voting: Doesn't have to be unique (multiple Masternodes can share the same voting key). It is used to cast budget votes.

The same keypair can be used for all three roles (at least for now, the operator key will be changed to a BLS key soon), but they must be different from the key of the collateral address.

2.3.3 New Transaction Type

Here in PIVX we introduce four new transaction types, each identifying a particular transaction payload, with its own validation rules:

- PROREG (*provider-register*): this is the main special transaction. Used for the registration of a new Masternode, setting all of its properties (such as the keys for each role). It creates the Masternode collateral, as one of its outputs, or it references a 10000 PIV unspent output on chain (in which case, it must include a signature with its keys, as proof of ownership).
- PROUPSERV (*provider-update-service*): sent by the mn operator to update the properties related to the service (IP address, operator payout address).
- PROUPREG (*provider-update-registrar*): sent by the mn owner to update the operator key, the voting key, or the payout address.
- PROUPREV (*provider-update-revoke*): sent by the mn operator to revoke the service, and put the mn in PoSe-banned state (e.g. in case of compromised keys). The Masternode can be "revived" later, by sending a ProUpReg tx, which sets a new operator key, and then a ProUpServ tx (signed with the new key), which sets the new IP address for the Masternode.

[18] https://github.com/dashpay/dips/blob/master/dip-0003.md

2.3.4 Code Architecture

Deterministic Masternodes are represented as objects of the class CDeterministicMN.

This class includes a member variable that stores a shared pointer to a constant CDeterministicMNState object, which encapsulates the DMN state (updated properties and status).

A list of Masternodes is represented by the class CDeterministicMNList, which uses immutable functional maps (https://github.com/arximboldi/immer) to hold the actual information about each entry.

A new list is built at every block and maintained by CDeterministicMNManager.

The use of immutable functional maps is an elegant solution, devised by Codablock, to reduce the memory overhead required for the Masternode list update at every block, by adopting a copy-on-write approach.

Immutable data structures are provided by default on functional-programming oriented languages, such as Clojure or Scala, but for C++ we currently need to rely on third party libraries. Future work could be explored looking towards an implementation based on std::maps, but that would severely impact the performance and require hundreds of MB in the ram, just for MN list housekeeping.

2.3.5 Masternode Voting on Budget Allocation

As a Decentralised Autonomous Organization[19] (DAO), PIVX operates and abides by its own community self-governance. No single entity, nor a small collection of aligned entities, possess the ability to dictate the direction in which PIVX grows. This organic approach to governance is intended to draw the most value from members of the PIVX community, who themselves act in their own collective best interest. One of the means through which this form of governance is obtained is through Masternode voting on monthly budget allocations. Currently, Masternode operators are granted the ability to vote on proposals made by community members with the intention of bettering PIVX, or circumstances for it, in some way. With well over 1800 Masternodes—which require a substantial investment into PIVX to operate—currently in operation, this approach greatly divides power, allowing for no absolute authority within the community.

2.4 Stakenodes

In principal, PoS has the same function as PoW, to reach consensus on the blockchain. However, as noted earlier, it's much less resource intensive, thus it has become the chosen method of consensus for PIVX and many others projects. Using the Proof of Stake model requires the users to invest in a node by *staking* (placing on) their coins/PIV on a node (core PIVX wallet). In return for staking users are rewarded a set amount of coins in return. Stakenodes or Validators are responsible for the same thing as miners in proof-of-work: ordering transactions and creating new blocks so that all nodes can agree on the state of the network.

Proof-of-stake and Stakenodes comes with a number of improvements to the proof-of-work system:

[19] https://www.investopedia.com/tech/what-dao/

- Better energy efficiency – you don't need to use lots of energy mining blocks lower barriers to entry.
- Reduced hardware requirements – you don't need expensive or specialized hardware to stand a chance of creating new blocks .
- Stronger immunity to centralization – proof-of-stake leads to more nodes in the network.

To run a Stakenode, users must simply be running the latest PIVX core wallet (on a device that will support its operation - laptop, desktop, raspberry pi, etc) AND have at least 1 PIV in their wallet AND have the wallet unlocked for staking.

3. GOVERNANCE

Community Designed Decentralized Governance[20] is the controlling feature of the PIVX DAO. As part of this system, there is an ability for proposals to be funded each month by the PIVX budget and Treasury. Proposals are submitted to the network by anyone to be voted on by the 2nd layer Masternodes. These node owners, located around the world, determine if the proposal should be funded.

3.1 Treasury Governance and Voting

3.1.1 Community Treasury:

Every month, the PIVX Treasury has a fixed amount of coins in free availability: 43,200 PIVs. These funds are allocated for the implementation of proposals that received a sufficient percentage of "Yes" votes in relation to "No" votes (~10%). For example, if there are 1,500 Masternodes, a proposal must have 150 (10% of 1,500) or more net Yes votes. (Yes votes minus No votes).

The PIVX Treasury is funded via one PIV per block added to the network. This generates a consistent available budget each cycle for the Treasury. These PIVs are not “created” per se, only allocated as *available* to be created/used. Proposals are submitted to the community’s system, voted on, and those proposals that are accepted are issued the funds they have requested.

This Treasury fund issuance occurs in a “Super Block”, which occurs every 30 days. Superblocks were created to work on seamlessly administrating the payment side of the Decentralised Voting Proposals. If a Proposal is voted in and confirmed, Superblock will appear at certain block counts and take care of all payouts automatically as confirmed by the code. This secures the decentralized system of the voting/payment process.

Superblocks work hand in hand with the budget system. In the first phase of the budget system, a proposal is prepared and submitted to the network. After 24 hours it is considered eligible, and can then be voted on. Once this occurs, it requires at least 10% of the network to vote yes to make it into the "budget projection". The budget projection is simply all of the proposals that qualify to get paid, sorted in order by {YesCount - NoCount} (the amount of Masternodes that voted Yes on a given proposal, minus the amount of nodes that voted No). As proposals are paid out, it continues until the budget system runs out of PIV for that payment period and will stop adding proposals to the projection. Subsequently, the PIVX network will take the budget projection and finalize it. At this point the rest of the Masternode network will compare their projection to the finalized budget and if they match they will vote "Yes". If more than 10% of the network votes yes on the finalized budget, then when the next super block is reached, the network will create these blocks. Superblocks simply pay one proposal per block until the budget per month is paid.

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 straightforward, 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 days x 24 hours a day x 60 minutes per hour x

[20] https://pivx.org/governance

1 PIV per block. 30x24x60x1 = 43,200 PIV allocated to the Treasury per Super Block. This forms the “budget” available for the proposals.

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 PIV available. 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.

Conversely, if the passing proposals exceed the 43,200 PIV allocation, proposals are funded in order of their yes votes until the PIV is exhausted. For example, if there are five passing proposals asking for 10,000 PIV each (50,000 total), only the first four will be funded with the remaining one not receiving funding. The protocol will only fund those projects that can be fully funded. Any remaining unspent funding is not carried forward and is never created. It is possible that exactly 43,200 PIV can fund passing proposals, with nothing remaining. However, this is rare.

3.1.2 Proposals Submission:

Anyone can submit their proposal for voting. Each proposal submission costs 50 PIV, which is burned. It doesn't matter how an individual contributes to the project’s development - as a designer, ambassador, singer, etc.

3.1.3 Decentralized Voting:

Masternode owners vote for the proposals put forward. This voting is decentralized and anonymous. Each Masternode owner has one vote per proposal per node they own.

3.2 Community Governance and Organization

As mentioned above, a system of proposals is submitted to the network (by anyone) to be voted on by the 2nd layer Masternodes. These node owners, located around the world, determine if the proposal should be funded.

There is another aspect to PIVX (not directly tied to the blockchain or Treasury payouts), that pertains to how the community (the individuals who choose to engage, participate, and work to help the greater PIVX economy and ecosystem grow) govern themselves and self-organize. These facets pertain to ancillary realms such as Discord, Telegram, and the like. In some instances, individuals submit proposals to seek funding to assume a role (such as social media coordinator, etc) in stewarding facets of the ecosystem. However, in most instances, individuals give freely and volunteer their time, talents, and energy in support of the larger PIVX vision.

The first guiding principle around which these individuals assemble is the PIVX manifesto, which states:

> *PRIVACY is non-negotiable. It's a basic human right.*

FREEDOM is everything.
TECHNOLOGY is advancing, GOVERNANCE must also.
Privacy ALLOWS the freedom to share what you wish with EVERYONE, but also the freedom to RESTRICT who sees your information.
We believe this is each person's CHOICE.
GOVERNANCE is used to further objectives and FUND development.
The DAOs are UNTOUCHABLE.
Join us WHEN you like, WHY you like, and, for AS LONG as you like.
Let's explore ALL the options TOGETHER.
You are IMPORTANT to US.
It's TIME we harnessed your FULL potential.

The other major (but loosely implemented) guiding principle of PIVX is the Swarmwise Methodology.[21]

> "It is an instruction manual for recruiting and leading tens of thousands of activists on a mission to change the world for the better, without having access to money, resources, or fame….based on Falkvinge's experiences in leading the Swedish Pirate Party into the European Parliament, starting from nothing, and covers all aspects of leading a swarm of activists into mainstream success.[22]"

Here are some of key skills for "swarmwise" leadership based on Falvinge's book:

1. Release Control

Releasing control is the first rule for swarmwise leadership. A swarmwise leader leads primarily through inspiration. Delegating authority can be scary, but for a swarm to function, all parts of it must become self-sufficient and autonomous. This is the only way to reap the cost-efficiency and execution-speed advantages of a swarm. To lead by releasing control, the leader must lead through inspiration and example, and empower anyone from within the swarm to step up and assume a role. This occurs organically; when a task or function is needed, no one assigns it; someone volunteers to lead it and inspires others to voluntarily follow. The swarm architecture allows for creating leaders on an as-needed basis; once a role, task or function is complete, the leader of that function ceases to lead. No one in the organization has an advantage over anyone else, and no one is assigned a role by anyone else; leadership happens naturally when a need is met with a talent.

2. Build a Culture of Leadership and Trust

In order for decentralized leadership to succeed, it must be supported by a culture of trust. The founder creates this culture for the organization, setting the tone and example and leading more as an archetype than as manager or mentor. Because this is the case, the founder and all leaders within the organization must maintain an excellent personal reputation, avoiding negativity and exhibiting values of patience, collegiality, passion, and understanding at all times.

[21] http://wiki.p2pfoundation.net/Swarmwise
[22] https://falkvinge.net/2013/02/14/swarmwise-the-tactical-manual-to-changing-the-world-chapter-one/

3. Observe the “Three-pirate Rule” for Decision-making

The “three-pirate rule” is a method of delegating decision making to the local area of the swarm where a decision is needed, expediting action and avoiding bureaucratic inertia. Basically, if three activists agree something is good, they do not need to ask permission of anyone to act in the name of the organization.

4. Define the Message, Leave the “Branding” to the Swarm

The leader of a swarm defines the content of a message and leaves it to others to figure out how to best convey the message given context and audience. There are no consistent messages, slogans or catchphrases, or style guides in a swarm. The same message can be delivered in myriad different ways to appeal to a local audience’s needs, values and characteristics.

5. Be the Media Face

The rest of the world needs an avatar to associate with the swarm, so it is important for a swarm leader to engage with the media in person, including all press appearances and major public events and rallies.

6. Build the Timeline

Members of a swarm need to understand where they are, where they are going and how they are going to get there. To achieve trust, the leader needs to set out a transparent timeline and identify key milestones that swarm members can understand, engage with, and feel a sense of accomplishment as milestones are reached.

7. Set visible, Active, Inclusive Goals

People are not attracted to a swarm for social reasons; they join a swarm because they believe in the mission of the swarm and want to accomplish it. To keep people engaged, goals must be identified that are inclusive and engaging. Measurement and gamification are ways to keep the swarm engaged and focused, and to tap into natural competition to get things done and achieve goals. To keep swarm members motivated, reward them with acknowledgement and attention—it’s a critical step to maintaining morale and faith. Swarm leadership increases the resilience of organizations; the swarm leader creates an ecosystem that is adaptable, redundant, and self-organizing. Ultimately, swarm leadership radically reduces bureaucracy by offering every member the chance to freely take initiative, participate, and lead according to their skills and interest level. "

4. FINANCIAL DATA PROTECTION

PIVX introduced the world's first zk-SNARKs based financial data protection protocol on a Proof of Stake blockchain in 2020, with mainnet activation live on January 30th, 2021. This protocol was given the name SHIELD, announced on November 5th, 2020.[23]

PIVX's implementation of SHIELD also represents anonymity to its users without individuals having to "mint" or create a different token to participate[24]. Instead, through the simplicity of selecting a "shielded" address, a user can send or receive PIV with the confidence that all data and financial records remain protected and anonymous. SHIELD provides complete privacy for your transactions, preserving the transaction details' invisibility from the sender to the receiver, the amount of the transaction, and balances.

SHIELD further provides the end-user with a robust and fast transaction experience. The lightweight *proofs* are as small as 144 bytes and can be generated in seconds, even on a low-powered computing device like a Raspberry Pi. Users can enjoy fast and secure/shielded transactions across the network that take less than 500 milliseconds to generate and 1/100ths of a second to verify.

As many projects have experienced (especially when requiring large denomination pools of "private coins"), the adoption and use are often small when privacy is opt-in. This puts the actual privacy of those who use the protocols in jeopardy as it makes it easier to identify those users and their funds. With SHIELD, anonymity through its shielded addresses is offered by default. However, the ability to operate in an unshielded manner (transparent) entirely remains, allowing end-users to work with exchanges.

4.1 Introduction to Zero-Knowledge Cryptography and zk-SNARKs

Zero-Knowledge proof is a cryptographic method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying (or unknowingly leaking) any information apart from one simple statement: that the statement being made is indeed true. A Zero-Knowledge protocol thus allows you to do something REALLY impressive, to prove that you know something without revealing what that something is.

Put another way, let's say you have knowledge of something, but can't share it with a second party outright due to security concerns. However, without verifying knowledge, how does this second party know that you know what you know. That's the very definition of "zero knowledge," no ("zero") information about the secret is revealed, but the second party (or any other party that needs to validate) is convinced (in full) that you know the information/data/details (that secret).

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKS) is a non-interactive zero-knowledge proof (ZKP) that can be verified without any interaction with the prover. The Sapling Protocol[25], makes use of zk-SNARKs proofs to allow both shielded and unshielded transactions on the

[23] https://pivx.org/news/introducing-shield-the-new-privacy-protocol-from-pivx
[24] https://z.cash/
[25] https://z.cash/upgrade/sapling/

blockchain, while Groth16[26] by Jens Groth, a SNARK construct created by a distributed multi-party computation setup phase, was used for the initial setup.

4.2 Sapling / zk-SNARKS (Groth16)

To start, zk-SNARK or, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, refers to a method of proof construction where an individual has the ability to prove possession of certain information (e.g., private key) without having to reveal that information to another party anonymously and thus not have any interaction. So, zk-SNARKS are a way to perform a "zero-knowledge" transaction – a proof that allows two parties to prove that a statement between a prover and verifier is true, nothing more. Sapling is an advanced privacy-enabling protocol developed by the Electric Coin Company[27], creator of Zcash[28], that combines all of the above technical aspects, along with a new cryptographic construction, standardizing a fully functional Decentralized Anonymous Payment[29] (DAP) scheme leveraged on a novel form of zero-knowledge cryptography called the Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKS). Sapling adds new highly usable types of transactions to the standard UTXO-based blockchain that enables the preservation of invisibility of transactional (meta) data while allowing the generation of zk-SNARKs proofs as small as 144 bytes within a matter of seconds on a low powered home computer. Thanks to this massive performance improvement in Sapling, private transactions become actually practical with <1 second (~500ms) needed to execute a private transaction. On the receiving side, it should take the recipient <1 second (~10 ms) to verify that transaction. These times place a private transaction into the realms of acceptable when it comes to large scale transaction and verification times for global commerce.

4.3 Sapling Keys

With Sapling, an individual generates what is called a "spending key," allowing them to perform a payment (what is the equivalent of having a secret/private key) and a "viewing key," which allows any individual who holds this key to see the payments received or emitted. This viewing key can be thought of then as a public "statement." For example, it can be shared with an escrow attorney/account, regulator, etc. for compliance purposes. However, you need not share the spending (or private key) to share the information.

Now, let's say you want to receive a payment. You can generate an address from that viewing key and relay that to the individual sending funds. What is really nice about Sapling addresses is that they are diversified. With a single viewing key you can create, or derive, a brand new address which in no way correlates to the previous one. How does this help maintain privacy? By having uncorrelated receiving addresses, an individual is thus prevented from potentially leaking identifiable information. If you use a static address, it would be possible for an entity to uncover the identity of the person being paid.

[26] http://www.zeroknowledgeblog.com/index.php/groth16
[27] https://electriccoin.co/
[28] https://z.cash
[29] https://ieeexplore.ieee.org/document/6956581

5. ECONOMIC MODEL

For a full writeup on PIVX's economic model and policy, please review the full whitepaper here[30].

The monetary policy of the PIVX project is designed to enable a sustainable infrastructure and service capable of supporting scalable, decentralized, and resilient node infrastructure. This will allow for instant and protected transactions globally, without astronomical Quantitative Easing[31] (QE) and the corresponding resulting devaluation[32] of the native token. This policy has had dire effects on other cryptocurrency endeavors, many using the PoS protocol.

5.1 Monetary Policy

PIVX's monetary policy will be dictated by how its primary economic levers are influenced and adjusted over time. Project mandates will ensure long term stability, sustainability and accessibility of the protocol. The monetary policy is specifically governed by the blockchain codebase, indirectly by the use of the network by its users, and controlled via the PIVX DAO via its protocol level governance model.

The primary economic levers managed by the monetary policy include, but are not limited to:

- Transaction Fee Cost and Burn.
- Rate of coin emission per block.
- Split of coin emission rewards per block between stakenodes and Masternodes.
- Minimum amount for staking.
- Requirements for Masternode.

5.2 Coin Economics

- PIVX has a fixed emission rate per block (every 60 seconds).
- 5 PIV as block rewards (2 PIV to Stakers, 3 PIV to Masternodes).
- 1 PIV is "allocated" (not created) to the budget/Treasury.
- PIVX relies on both stakers and Masternodes to possess its native coin, PIV or $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. Staking profitability decreases with the increase of the total amount of coins being staked, and Masternode profitability decreases with the rise of the network's active Masternodes.
- 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 essential 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.)
- The annual PIVX inflation rate is currently around 4%, with a slight and steady decrease over

[30] https://pivx.org/whitepaper
[31] https://www.investopedia.com/terms/q/quantitative-easing.asp
[32] https://www.theglobeandmail.com/report-on-business/rob-commentary/quantitative-easing-is-just-devaluation/article1391719/

time as the block's emission rate 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.

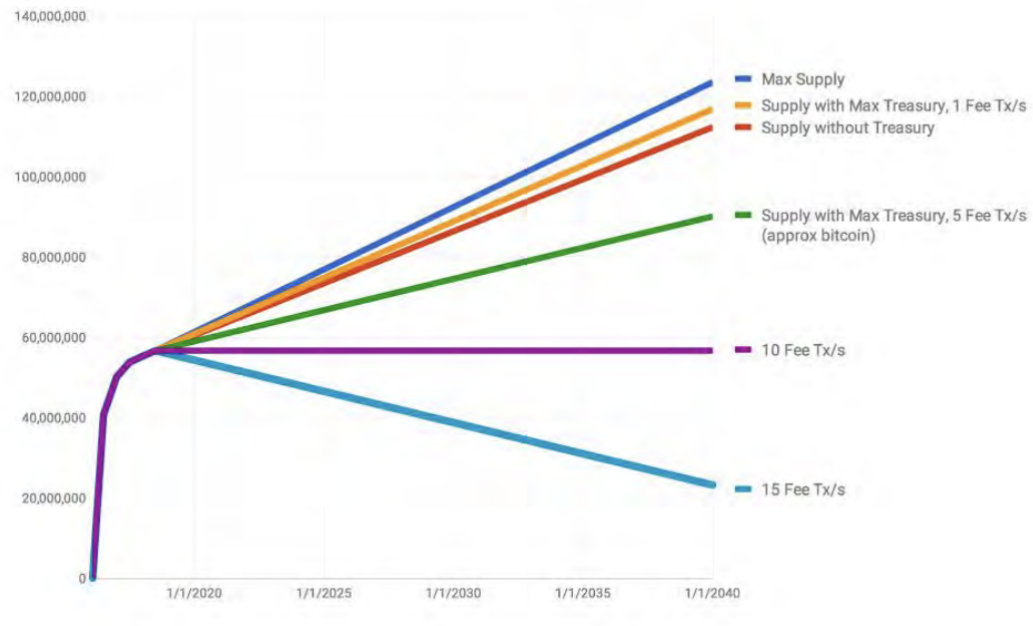
5.3 Maximum Coin Supply

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 2040: 125,929,497 PIV.
- By June 2060: 189,001,497 PIV.

5.4 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 currency[33]-[34], 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. There also exist options 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.

[33] https://archive.org/details/encyclopediaofba00woel/mode/2up?q=elastic+currency
[34] http://www.eagletraders.com/advice/securities/elastic_currency.php

6. FUTURE CONSIDERATIONS

6.1 Beyond Trusted

Although it's too early to be certain of the exact construct that will be used in the future, and while Sapling's large 88 participants[35] multi-party computation (MPC)[36] is assumed highly secure in its construct, PIVX will strive to achieve a trust-less setup of Sapling in the near future; post initial implementation. Some trust-less constructs being researched currently for this are Halo[37], Spartan[38], and SuperSonic[39]. What this means is that PIVX is aiming to remove the reliance on a trusted cryptographic proof that was created by random participants, in order to achieve a trustless zk-SNARKs proof setup, leading to post-quantum resistance before they become a significant risk.

6.2 PIVX's Environmental Impact

While admittedly not an original goal of the PIVX project, the collective organization has realized that the domain of cryptocurrency has pushed the environmental boundaries upwards and outward from where we started in 2015. With the normalization of carbon offsetting in the business world, PIVX has moved to not only become the first cryptocurrency project to become carbon neutral, but to also be the first to cover all of its years in existence. PIVX is currently working with Regan.Network[40] to incorporate our shared vision of offsetting Greenhouse gas emissions created by the node operators and users of the project. As of this publication date, PIVX has become what we believe to be a necessary; a Net-Zero CO_2 Project.

6.3 Private staking

PIVX is no stranger to Private staking, having been the first ever cryptocurrency to deploy private staking (with the prior, now deprecated, zPIV / Zerocoin Protocol implementation) into PIVX's proof of stake blockchain.

PIVX will introduce a brand-new SHIELD staking feature. It will allow an individual to stake shielded coins and receive the staking rewards directly to a shield address. This feature will protect users' data, uphold their financial data protection, and increase the shielded coins' percentage in the PIVX network, further strengthening the SHIELD protocol.

[35] https://github.com/ZcashFoundation/powersoftau-attestations
[36] https://electriccoin.co/blog/new-mpc-protocol/
[37] https://eprint.iacr.org/2019/1021
[38] https://eprint.iacr.org/2019/550
[39] https://eprint.iacr.org/2019/1229
[40] https://www.regen.network/

6.4 Decentralized Autonomous Stake Pools (DASPs)

The idea of a "pool" comes from PoW. In PoW, you can mine either directly (similar to how PoW was, back in the Satoshi days) or join into a "conglomeration" of miners, called a Pool (which is how the vast majority of PoW coins are mined). In PIVX, we are basically "solo staking" now (similar to solo mining PoW). A staker will only get the block reward if they find a valid block (in which case they are awarded the full staker-portion of the block reward, i.e. 2 PIV). With pools you don't need to find a winner block, you just provide hash-rate (in the case of PIVX: staking power). When a block is found by the pool, the pool operator takes his cut and allocates the remaining part in a "rewards pool". Every X blocks (e.g. once a day) the pool operator distributes to the stakers the funds accumulated in the rewards pool, percentually based on how much staking power was provided by each one. However, in this case, the stakers need to trust the operator with the new rewards (same as PoW miners do, when they point their asics to a mining pool). The idea of a "trustless" pool (or rather DASP "decentralized autonomous" staking pool) is to remove this centralization element by allowing any full-node staker to participate (and compete) as pool operator, and by making the rewards distribution verifiable by consensus (enforcing the payment at specific heights, same as we do with superblocks).

6.5 Governance Evolution

A significant amount of time and research has gone into exploring what the next evolution of PIVX's DAO governance could look like. A full compilation of those investigations can be found here,[41] Title under "Community Designed Governance."

Four different proposals and hypothesis were put forward:

1. PIVmetheus
2. Weighted Voting System
3. Votes-For-All Consensus Proposal
4. Tango

Each proposal covers different approaches at a more robust, involved, and community centric governance scheme. While it is outside the scope of this White Paper to go into depth about each, we highly encourage those interested in the future of PIVX governance to explore these 4 proposals.

[41] https://github.com/PIVX-Project/CDG

7. ACKNOWLEDGMENTS

PIVX derives itself from countless ideas, dreams, and vision that existed before its inception. The vision of a decentralized, rights preserving, digital means of exchange and value transfer was discussed even by Milton Frieddman in 1999[42]. There are many individuals who must be given considerable credit and thanks. Without the help of many brilliant people, PIVX would not exist. Notwithstanding, especially the current "team" of individuals supporting and growing the PIVX ecosystem as a whole, be they developers, social managers, community sherpa, business developers, and beyond. This group of individuals, many of whom volunteer their time and efforts, are what keep PIVX moving forward.

Specific to this whitepaper, a special thanks to the individuals below:

Ambassador - Proofreading and content suggestions
Eric Stanek - Proofreading and content suggestions
leacy mck - Proofreading
AzerX - Proofreading
Chris Khoury - Proofreading
Sigge B - Proofreading

[42] https://www.youtube.com/watch?v=9Vw2_Onfe6M