PIVX

White Paper

Version 1.01a, September 2018

Written and Compiled by Strontium

Contributors

presstab, warrows, Rhubarbarian, Sieres, CryptoHB, s3v3nh4cks, random.zebra

Input/Support

Eric_Stanek, Fuzzbawls, SnappySnap, Cryptosi, gets, thuggins, John M, Buer, Evan, deejayem, Rock-N-Troll, Mary, turtleflax, furszy, mcl4m

ABSTRACT

Currently, the cryptocurrency market is awash with tokens from parties of varying intent, motivation, and affiliation. The myriad of tokens and projects—some novel and ambitious uses of blockchain, others in essence clones with catchy names—serves as a deterrent to widespread adoption of crypto as a legitimate, borderless alternative to fiat currency. This document serves as a comprehensive resource on the ***Private Instant Verified Transaction*** *(PIVX) cryptocurrency, a currency whose defining purpose is to provide users with a fast, secure, private, and stable means of transacting over the web. PIVX integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology; speed and governance accessions from Dash, such as SwiftX (from InstantSend) and a Masternode network; and incentivises Zerocoin protocol anonymity through zPoS. PIVX also incorporates its own features, such as a Proof of Stake consensus algorithm, and a dynamic coin supply restrained by the burning of transaction fees.*

Note that this paper, while an extensive introduction and explanation of PIVX, does not contain mathematical or cryptographical breakdowns or explanations. These can be found separately on the PIVX project's GitHub.

TABLE OF CONTENTS

1 INTRODUCTION

The advent of the blockchain era occurred in 2009 with its implementation in *Bitcoin* by the entity known as Satoshi Nakamoto. Following Bitcoin's success, many competing cryptocurrencies—known as *altcoins*—have arisen. The potential of blockchain to revolutionise not only the way transactions are made, but the way business is conducted across many strata, has seen an explosion of interest in the technology. Currently, the cryptocurrency market is awash with tokens from parties of varying intent, motivation, and affiliation. The myriad of tokens and projects—some novel and ambitious uses of blockchain, others in essence clones with catchy names—serves as a deterrent to widespread adoption of crypto as a legitimate, borderless alternative to fiat currency.

Bitcoin, despite its constant innovation, has so far 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. As the world approaches a decade since the launch of Bitcoin, a definitive identity for cryptocurrencies has yet to emerge. This lack of identity has caused the public to view the crypto marketplace as a stock market 2.0. Its 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 bridge the gap between the tech-savvy and tech-wary. It strives to provide a safe means through which not only investors, but the general public can conduct business without the need for financial institutions or middle-men. PIVX's aim is to provide the people of the ever more interconnected world with an expedient, private means to conduct business on their own behalf.

1.1 PRIVATE INSTANT VERIFIED TRANSACTION

The **Private Instant Verified Transaction** (PIVX) cryptocurrency (formerly DNET), is a currency whose defining purpose is to provide users with a truly private means of expediently, securely, and stably transacting over the web. PIVX integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology; speed and governance accessions from Dash, such as InstantSend and the Masternode network; and features the addition of the anonymity protocol Zerocoin on transactions and staking—all of these heavily customised. PIVX also incorporates its own features, such as a Proof of Stake consensus algorithm, the ability to stake both PIV and zPIV, and a dynamically calibrated coin-supply restrained by the burning of transaction fees.

- *For more on zPIV see section 6.2.*

PIVX is ***DECENTRALISED***, ***INCENTIVISED***, and ***OPEN-SOURCE*****.** 60-thousand 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, and no amount of PIV is locked away in order to manipulate the PIVX economy.

As a **Proof of Stake** cryptocurrency, PIVX is significantly **better for the environment** than Proof of Work focused cryptocurrencies due to its lower energy consumption requirements.

Zerocoin Proof of Stake (***zPoS***) allows for PoS rewards to be earned while maintaining and incentivising anonymity.

- *For more on zPoS see section 6.*

PIVX transaction and zPIV minting fees are burnt, and new coins enter at a predetermined rate, thus managing the coin supply and protecting against hyperinflation.

Approximately 16.66% of block rewards are used as treasury to fund the further advancement. The PIVX blockchain pays out this funding via *superblocks* monthly, through which the self-governed community budget out software development, as well as marketing, translation, QA, *etc*. via voting.

- *For more on fee burning see section 2.2.*
- *For more on budget and self-governance see section 4.2.*

1.2 VISION/MANIFESTO

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.

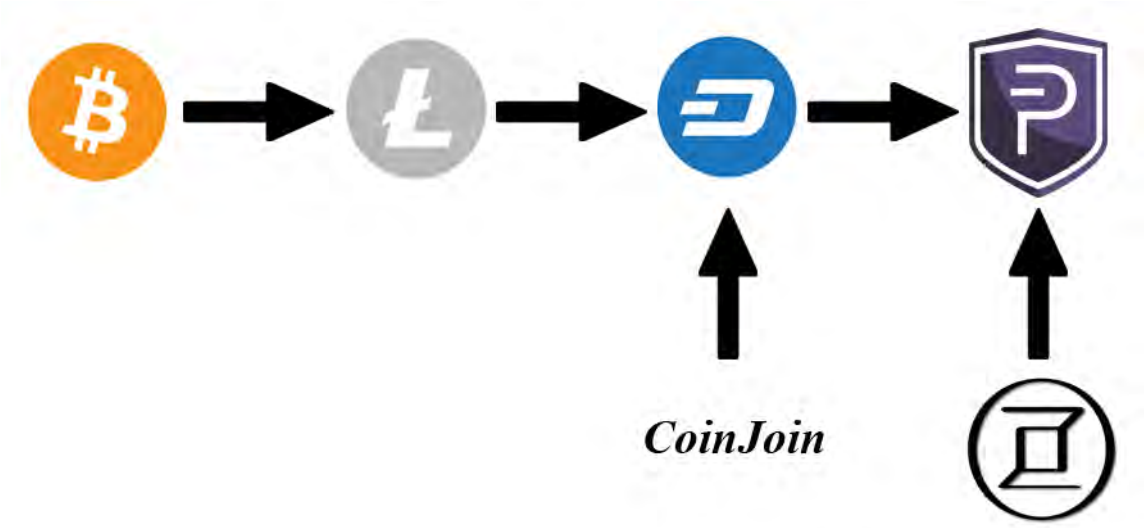
The DAOs are untouchable.

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.

2 ANATOMIC OVERVIEW OF PIVX

As PIVX exists with the purpose of becoming the quintessential privacy-based currency, its base features are an aggregate of those pre-existing in other currencies. These have been tailored and added to in order to provide a single currency able to perform with the strengths of these currencies without their weaknesses. Beyond this, PIVX, and the untraceable zPIV and Zerocoin protocol, possess further features that set PIVX apart from its predecessors and contemporaries.

The software technology behind PIVX is drawn from a lineage of successful cryptocurrencies, with each having sought to improve upon those before it. PIVX, which started as a code *fork* of Dash, can draw its root back from there to Litecoin—from which Dash was forked—and back to Bitcoin (it's worth noting that Dash returned in large to Bitcoin codebase before the PIVX fork). All three of these coins have spent time in the top 10 cryptocurrencies.



• *A demonstration of the flow of tech from Bitcoin forking to Litecoin; Litecoin forking to Dash, implementing CoinJoin; Dash forking to PIVX, implementing Zerocoin.*

PIVX is constantly working to improve upon not only these previous technologies, but upon its own. As such, features once implemented by PIVX, such as the early PoW phase, CoinJoin, and the retired Seesaw mechanism make way for more ambitious features.

2.1 PIVX COIN SPECS

PoW Phase Period: January 30th 2016 to August 17 2016 (FINISHED)

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

Block size: 2 MB

Block Time: 60 Seconds (Re-targeting every block)

Coin Emission Rate: Max. 6 PIV per block (Always less due to burnt fees & unused treasury). 5 PIV are allocated as staking/masternode rewards, and 1 to superblock budget payout.

Coin Supply Control: ALL transaction & zPIV minting fees are burnt from coin supply.

Maximum Coin Supply

At June 2018: 56,550,297 PIV
By June 2020: 62,857,497 PIV
By June 2040: 125,929,497 PIV
By June 2060: 189,001,497 PIV
Theoretical maximum. Will actually be lower due to fee burning + partial budget generation.

PoS Stake Eligibility

Minimum Input Age: 60 blocks
Reward Maturity Confirms: 101 confirms
Wallet Status: Requires wallet to be kept running & online.

Transaction Send Eligibility

Minimum Confirm: 6 confirms

SwiftX Eligibility

1 confirm for locking and 6 confirm to spend.
Collateral held for 15 blocks.

Privacy Technology: Custom Zerocoin Protocol based on libZerocoin (we call this zPIV)

Key Features: Custom accumulator check-pointing system

Accumulator Modulus: RSA-2048

zPIV Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000

Mint time: >= 0.5 seconds

Spend time: >= 2.5 seconds

Maximum single Spend limit: 35,000 PIV

Maximum single Spend denomination count limit: 7

Fees (mint): 0.01 PIV per minted zPIV denomination.

Fees (spend): No fee to spend zPIV back to PIV.

Minimum PIV confirmation count required to mint zPIV: 6 confirmations

Minimum zPIV confirmation count required before spend: 20 confirmations

Maturity requirement before zPIV can be spent: 1 new identical denomination mint added to accumulator

Initial Masternode Coins: (now burnt & no longer exists in coin supply)

[block# 000001] 60,000 PIV for creation of 6 Masternodes for the functioning of the network.

[block# 279917] 60,000 PIV was publicly burned at block 279917.

- *For more on zPIV and the PIVX Zerocoin protocol see section 6.*

2.1 PIVX COIN SPECS CONT.

PROOF OF WORK PHASE REWARDS BREAKDOWN

Block height	Masternodes	Miner	Budget
2-43200	20% (50 PIV)	80% (200 PIV)	N/A
43201-151200	20% (50 PIV)	70% (200 PIV)	10% (25 PIV)
151201-259200	45% (22.5 PIV)	45% (22.5 PIV)	10% (5 PIV)

PROOF OF STAKE PHASE REWARDS BREAKDOWN

Phase	Block height	Reward	Masternodes & Stakers	Budget
Phase 1	259201-302399	50 PIV	90% (45 PIV)	10% (5 PIV)
Phase 2	302400-345599	45 PIV	90% (40.5 PIV)	10% (4.5 PIV)
Phase 3	345600-388799	40 PIV	90% (36 PIV)	10% (4 PIV)
Phase 4	388800-431999	35 PIV	90% (31.5 PIV)	10% (3.5 PIV)
Phase 5	432000-475199	30 PIV	90% (27 PIV)	10% (3 PIV)
Phase 6	475200-518399	25 PIV	90% (22.5 PIV)	10% (2.5 PIV)
Phase 7	518400-561599	20 PIV	90% (18 PIV)	10% (2 PIV)
Phase 8	561600-604799	15 PIV	90% (13.5 PIV)	10% (1.5 PIV)
Phase 9	604800-647999	10 PIV	90% (9 PIV)	10% (1 PIV)
Phase 10	648000-1153159	5 PIV	90% (4.5 PIV)	10% (0.5 PIV)
zPoS Phase 1	1153161-Onward	6 PIV	83.33...% (5 PIV)	16.66...% (1 PIV)

2.2 PIVX ECONOMICS

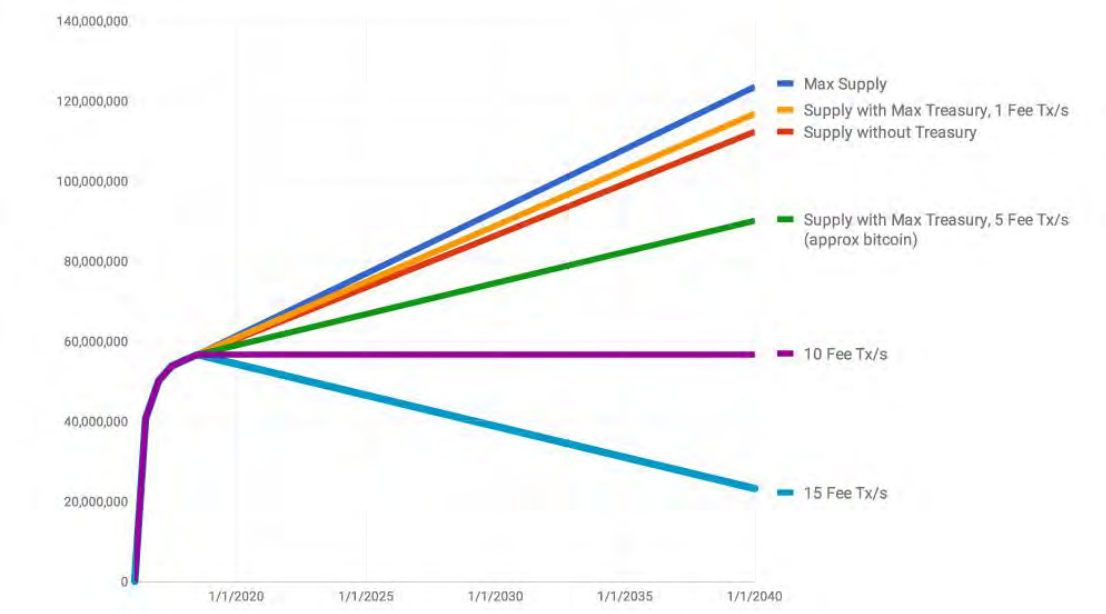
PIVX, with its intended purpose as a currency, is by design lacking a coin-supply limit. To maintain the health of the ***dynamic coin supply***, **PIVX burns its transaction fees.** The intention is to encourage liquidity and to reward users for participating in the network. A *hard cap* will never be reached to prevent the minting of new PIV, and so block rewards will continue to go to those securing the blockchain. This prevents the need to increase transaction fees, thusly supporting the liquidity vital for PIVX to function as a currency.

PIVX now issues about 5 PIV into circulation every minute (6 in total, but treasury allocation and *unspent allocation burning* decreases this), which is approximately a 4% inflation rate (though contentious, a figure often given as the sweet zone for providing new currency into circulation without triggering hyperinflation is 2-4%, though this figure applies to fiat currencies).

- *For more on block rewards see section 5.*
- *For more on inflations see section 2.2ii.*

2.2 | 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 burn)s. 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*, 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.[1]

[1] http://www.eagletraders.com/advice/securities/elastic_currency.php

2.2 I DYNAMIC COIN SUPPLY CONT.

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 values is not a simple number to predict, however, as fees vary. For example, compared to standard PIVX transactions, SwiftX transactions are more fee-heavy, and the minting of zPIV has a flat fee of 0.01 PIV per denomination. There also exist options within the PIVX Core wallet to opt for *custom fees*, with the ability set them higher than default; or a slower, *feeless transaction*. These variables make giving a flat transaction rate per block on the neutralising effect impossible.

- *For more on SwiftX see section 4.1 i.*
- *For more on zPIV see section 6.2.*

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. As block time target is 60 seconds with PIVX, the economy is maintained by the minute, daily. Following are maximum coin supply projection based on the current PIVX coin supply algorithm:

At June 2018: 56,550,297 PIV
By June 2020: 62,857,497 PIV
By June 2040: 125,929,497 PIV
By June 2060: 189,001,497 PIV

Theoretical maximums. Will actually be lower due to fee burning + partial budget generation.

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

- *For more on the decentralised government see section 4.2.*

2.2 II INFLATION/DEFLATION

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, 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.

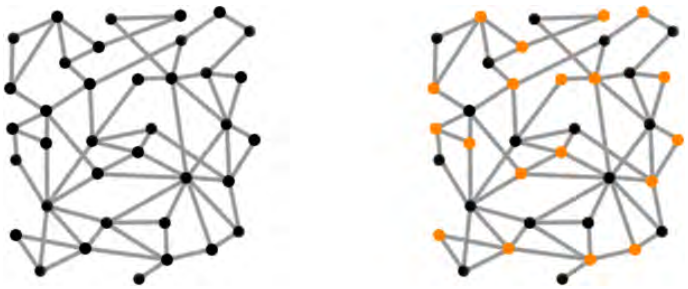
With the PIVX network emitting PIV with each new block, inflation may initially seem a concern. It's important to note, however, that **the PIVX economy is very different from those based on money or fiat currency**. Unlike gold or silver coins, PIV are divisible, and cannot be debased, so maintain fungibility. 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.

2.3 BITCOIN/LITECOIN ROOTS

The progenitor of all cryptocurrencies, Bitcoin was the first implementation of blockchain ledger technology. It serves as a means to maintain a distributed, immutable ledger by which peer-to-peer transactions can take place without an intermediary. As it is decentralised, Bitcoin does not rely on any one point or authority for its operation or maintenance, but rather operates on a network of nodes, with the network itself verifying transactions taking place within it. These fundamental properties of Bitcoin have been carried over into PIVX. Although PIVX's direct predecessor, Dash, started as a Litecoin fork, it switched to Bitcoin before the PIVX fork, though some development additions from the time using Litecoin codebase carried over.

Bitcoin and Litecoin rely on the processing power of *mining* computers in the network in order to maintain the integrity of the ledger. Transactions are recorded into data chunks, each of which is called a *block*. The ledger, orchestrated as a chain of blocks—hence blockchain—counts on the processing power of the mining computers to solve a cryptographic puzzle by identifying an arbitrary number (*nonce*) to hash with. This reliance on mining is known as a *Proof of Work* (PoW) system. As the network grows, these cryptographic puzzles increase in difficulty, becoming harder to solve and drawing more processing power.

Unlike Bitcoin and Litecoin, PIVX does not rely on PoW. A critical issue with Proof of Work systems is that they highly incentivise *mining pools*—groups of computers working together to solve block hashes and share in the reward to circumvent increasing processing requirements to remain competitive. This approach leads towards the processing power of mining pools pushing out individual miners. This method fundamentally slows the network as it grows, and also consumes a great deal of energy so negatively impacts the environment.

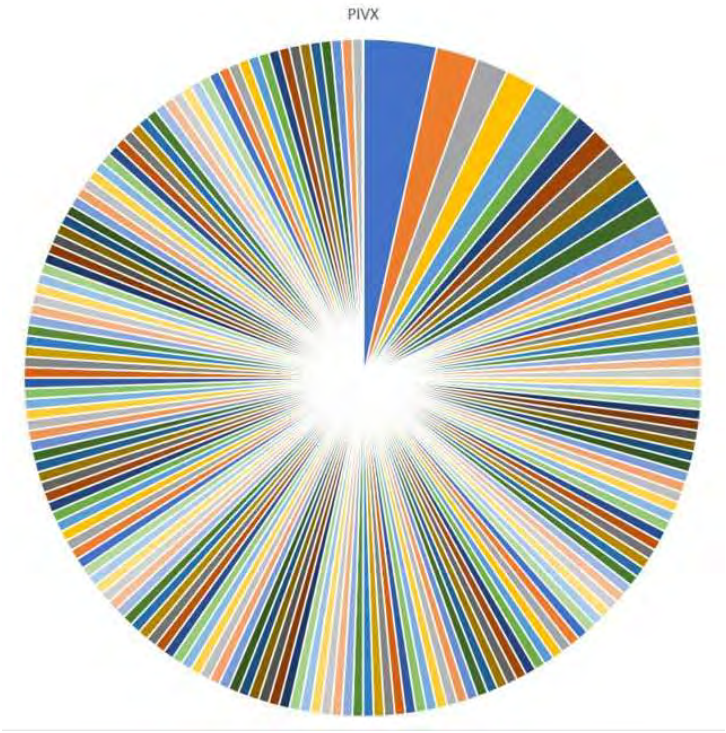


• *If in the above network representations black nodes are individual miners, those on the left could expect a relatively fairly distributed mining reward with similar processing power. The right diagram, whose orange nodes pool efforts and distribute rewards among pool members, throws off the mining reward balance.*

2.3 BITCOIN/LITECOIN ROOTS CONT.

It should be noted that Litecoin, with its use of the *scrypt* algorithm, is faster to hash a block than Bitcoin, but the cost of mining devices for such mining is more limiting[2]. With the arrival of ASICs (Application-Specific Integrated Circuits) miners, for both SHA-256 and Scrypt based PoW blockchains, the possibility of centralisation, and the danger it brings is even more apparent.[3]

Though eschewing PoW, PIVX continues to utilise the fundamental methodology of blockchain ledger consensus, with desirable Bitcoin updates being incorporated into PIVX soon after Bitcoin implementation.



The above image represents PIVX addresses receiving staking rewards over a period of 100 blocks. While it is possible some of these addresses are controlled by the same wallet, the likelihood is that the vast majority are operated by different PIVX users, each supporting the integrity of the network.

- *To read about PIVX's alternative to the PoW reward system see sections 3, 4, and 5.*

[2] Coventry, A., *NooShare: A decentralized ledger of shared computational resources*, 2.1.1, 2012, http://web.mit.edu/alex_c/www/nooshare.pdf
[3] Lee, C., *Charlie Lee [LTC],* https://twitter.com/satoshilite/status/857374260226007040?lang=en

2.3 | SCRYPT AND X11 MINING ALGORITHMS

In its PoW phase, PIVX utilised the Quark algorithm as it was deemed most fair due to its less exclusive technical limitations. Quark was, however, shed with the shift to PoS.

Scrypt is a key derivation function used as a mining algorithm. Its inflated memory costs serve as a defense against custom hardware attacks such as those seen from ASICs, which became increasingly necessary in order to profitably mine Bitcoin and other higher value coins several years into cryptocurrency's existence. It did not take long for Scrypt-specific ASICs to be developed for the mining of Scrypt dependent cryptocurrencies.

X11 was developed in 2014 as a more energy efficient hashing algorithm. By using a system composed of eleven separate rounds of hashes, X11 proved resistant to ASICs for a short time. The ease and energy efficiency of X11 once again allowed a larger user-base to mine until such a time as targeted hardware became widespread, effectively locking out those relying on non-specific hardware such as GPUs.

PIVX, having moved to proof of stake for consensus, avoids complications associated with ASICs by limiting hashing attempts dependent on UTXOs.

- *For more on Proof of Stake consensus see section 3.*

2.4 DASH ROOTS

Dash is an altcoin focused on speed, and once focused on privacy. Dash is the direct predecessor of PIVX. Dash takes a pivotal leap away from Bitcoin, and Litecoin from which Dash was *forked* from, by allocating *masternodes*. In the Dash network, masternodes are nodes crucial to the operation of the network. They are by necessity nodes in the network that provide maximum uptime and service. Running a masternode requires the node locks 1000 Dash, and is rewarded with dividends from an approximate 45% of block rewards. The design of the masternode system assumes that any one entity attempting to accumulate and lock out sufficient Dash to compromise the decentralised nature of the masternodes will cause the market price to rise in response, limiting such efforts.[4]

This inclusion of masternodes in the network makes Dash a two-tiered rather than single-tiered network. While miners remain responsible for the creation of new blocks, masternodes handle other integral services.

- *For more on masternodes see section 4.*

2.4 I PRIVATESEND

PrivateSend is a *coin-mixing* feature of Dash based on *CoinJoin*. *Coin mixing*—also known as *tumbling*—involves the obscuring of a transaction via the dividing of funds to protect their source. Not moving the sum total of a transaction directly from source to target, but rather complicating it via dividing it into mixed transactions, makes it much more difficult to track any one mixed transaction. This process serves to maintain the fungibility of units of the currency.[5]

[4] Based on information from Dash Whitepaper: Duffield, E., Diaz, D., *Dash Whitepaper, Section 2 Masternode Network*, https://github.com/dashpay/dash/wiki/Whitepaper
[5] *ibid*., *Section 3 PrivateSend*

2.4 I PRIVATESEND CONT.

Dash improved upon the CoinJoin methodology by allocating the task of coin-mixing to masternodes rather than focusing it at a single location within the network, removing a potential vulnerability. This allows mixing to take place using multiple masternodes, further increasing privacy on a transaction.[6]

PIVX, too, utilised its own improved upon version of CoinJoin, but has since innovated beyond it (as of Core wallet version 3.0.0) to further increase privacy via the Zerocoin protocol.

- *For more on the PIVX Zerocoin protocol see section 6.*

2.4 II INSTANTSEND

By utilising the masternodes, Dash allows for near instantaneous transactions. These transactions are allocated to, and handled by masternodes by quorum consensus. This allows for transactions to be locked in, allowing only non-conflicting transactions or blocks to proceed on the blockchain.[7]

PIVX shares a similar feature, called SwiftX, giving PIVX the same reliable, speedy transaction times Dash manages.

- *For more on PIVX's SwiftX see section 4.1i.*

[6] *op cit*. Dash Whitepaper, Section 3.
[7] *ibid*., Section 4, *Instant Transactions via InstantSend*.

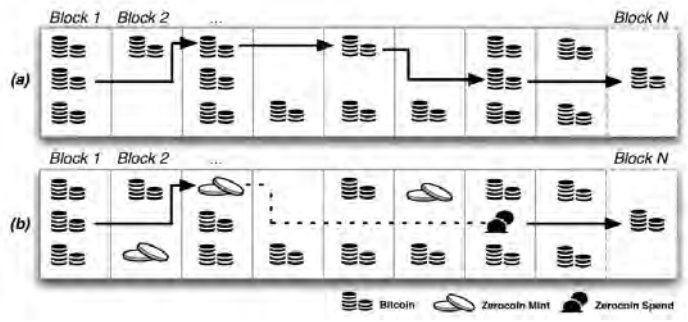
2.5 LIBZEROCOIN

Zerocoin is a protocol based on the ***Zerocoin: Anonymous Distributed E-cash from Bitcoin*** paper released by the John's Hopkins University (*see citation 8 for details*). It was proposed as an evolution of cryptocurrency privacy, moving away from coin mixing to a more secure, anonymous system.

LibZerocoin—the Zerocoin Project—is a Github hosted C++ library developed by The Johns Hopkins University Department of Computer Science. It was developed as a practical C++ implementation of the Zerocoin concept for giving Bitcoin transactions privacy, which the developers felt it was sorely lacking.

- *The logo and name of the Zerocoin protocol as it appears on the website. The Zerocoin website can be found at* http://Zerocoin.org/ *— the libZerocoin Github is found at* https://github.com/Zerocoin/libZerocoin

Zerocoin works by interspersing a second, private currency alongside the *basecoin* (original currency type) within blocks. These private Zerocoins are minted, their origin obscured, and added to the block to be later spent without revealing the destination or amount, essentially leaving no trace.



- *These diagrams depict a standard Bitcoin transaction (a), and one with Zerocoin protocol added (b). The dotted line, which follows the minted Zerocoins until spent, cannot be traced by observing blockchain data.*[8]

[8] (Image and basic explanation) Miers, I.,Garman, C., Green, M., Rubin, A.D., *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, The Johns Hopkins University Department of Computer Science, Baltimore, USA. http://Zerocoin.org/media/pdf/ZerocoinOakland.pdf

2.5 LIBZEROCOIN CONT.

To use the PIVX implementation of Zerocoin as an example, when minting zPIV, the process sees the user spend PIV to public accumulators. This burns the PIV, and in return the user receives an I.O.U.— stored by the user via their zPIV seed, and not tied to an address via the blockchain. A period of time is allowed for maturing, in which an additional zPIV mint of the same denomination is necessary before a spend is possible; this serves as a measure to ensure transactions cannot be traced back to addresses via comparative analysis of spends and mints, and to maintain a healthy zPIV pool size. Once this time passes, the user can redeem their I.O.U. via a spend with the zPIV spend's target address then receiving freshly minted PIV with no transactional history or origin.

The necessary files and information to compile the Zerocoin library are hosted for the purpose of distribution to the public not for use as a complete product, but an incomplete one the developers openly state is unfinished and inevitably buggy. It remains available largely as it was—mostly abandoned as a proof of concept. For this reason, it would be unwise for any team to simply introduce the protocol as is into an existing project.

PIVX has taken the unfinished Zerocoin protocol, available as libZerocoin, and further developed and bug-fixed it in order to produce the zPIV accumulators. While the PIVX Zerocoin protocol has libZerocoin as a basis, a great deal of altering of the Zerocoin protocol was necessary in order to properly accommodate it into PIVX's Proof of Stake network. PIVX is thankful for the early work of the Zerocoin developers, which PIVX has developed into its own, fully realised Zerocoin protocol and vital part of its identity.

- *The zPIV logo, which marries the 'z' from Zerocoin, and PIV—the standard unit of PIVX. For more on zPIV and the PIVX Zerocoin protocol implementation see section 6.*

2.6 PIVX INNOVATIONS

This section highlights some of PIVX's innovations, as well as giving insight on the foreseeable implementation strategy of PIVX. Notes directing the reader to the appropriate section of this document for more information where applicable can be found trailing paragraphs.

The **two-tiered PoS network** enables anyone the potential to earn additional PIV. While the cost of a masternode may have become unrealistic to many, the option to stake and earn staking rewards means new adopters have the potential to earn immediately. The likelihood of earning staking rewards is dependent on wallet balance, with that potential and frequency growing the more PIV is staked.

- *For more on staking and reward balance see sections 3 and 5 respectively.*

zPIV are PIV that utilise the Zerocoin protocol to maximise privacy for the user. Whether to use zPIV or not is the choice of the user, though **zPoS (zPIV staking)** provides higher staking rewards, and added privacy on transactions.

- *For more on zPIV and the Zerocoin protocol see section 6.*
- *For more on staking reward potential to wallet balance see section 3.*

The **dynamic coin supply** of PIV exists as a unique means of ensuring the health of the PIVX economy. This is handled by the blockchain rather than any individual or group, with tweaks being possible upon community consensus in the event any tuning beyond the fee-burning adjustment algorithm becomes necessary.

- *For more on the dynamic coin supply see section 2.2 i.*

PIVX is always working on new features to improve, with the implementation of groundbreaking technology taking precedence. Multiple new features are always being worked on at any given time, be they angled towards improved privacy, speed, or adoption.

2.6 PIVX INNOVATIONS CONT.

The following are features currently being developed as natural progressions of those previously listed. ***Note*** *as these features are in development, in some cases, further technical or release details cannot yet be shared, as they are subject to change*.

zDEX, a decentralised exchange, will rely on zPIV to ensure privacy with transactions. It will allow the purchase of PIVX without the need to involve a centralised platform as a medium.

> The idea behind launching zDEX is to give people a way to access PIV absent the need to utilise an exchange. In doing so, users will be spared the trouble of additional steps when accessing PIV, as well as spared the fees and wait times associated with those steps. Note that for countries that tax cryptocurrency on a per-transaction basis, it will be up to the individual to record zDEX transactions, as the use of the Zerocoin protocol for zDEX makes record keeping impossible, as well as in violation of the zPIV privacy principles.

- *For more on zDEX see section 6.4.*

Bulletproofs are set to improve the efficiency of the PIVX Zerocoin implementation. *Details can be found in section 6.1 of this document*.

I2P network integration aims to further improve privacy of PIVX transactions using a fully decentralised peer-to-peer network.

> I2P serves as an improved alternative to TOR, working to further sever traceability of PIVX network activity. I2P features a range of technical advantages over TOR and similar models, while providing added speed, robustness, and security.

Dandelion Protocol—designed initially to add privacy to Bitcoin transactions—to add an additional layer of privacy to the already outstanding privacy PIVX Zerocoin provides.

> The Dandelion Protocol, designed to add privacy to Bitcoin transactions, protects the IP address of the sender through relaying a transaction across nodes in the stem phases, then dispersing it to multiple nodes in the fluff phase. This makes tracing the origin of the transaction exceedingly difficult. This extra measure of privacy, stacked with those already extent and planned, is intended to give PIVX users peace of mind when transacting.

Other innovations are always being worked on, but these above serve to highlight the natural progression of PIVX following the current zPoS phase.

2.7 DEVELOPMENT AND RELEASE PRACTICES

PIVX is a decentralised project developed, run, and maintained by the community. Development is funded by the DAO via the monthly budget as voted on by masternodes, though anyone is able to view, make suggestions on, or learn from the PIVX source code. The PIVX project extends beyond the PIVX Core wallet, also including such projects as the PIVX Android wallet, iOS wallet, Secure PIVX Masternode Tool, and other PIVX-related projects.

- *For more on the PIVX DAO and PIVX governance see section 4.2.*

PIVX development and releases are handled using GitHub. Standard software version control and management practices are followed using the PIVX repositories. Linus's Law applies ("*Given enough eyeballs, all bugs are shallow*") as the repositories are open to numerous developers and testers during development, though public eyes are generally not permitted access until the product in question reaches a release-ready state.

As of early 2018, software developed under the PIVX project is subjected to extensive QA testing prior to public release. QA testing includes, but is not limited to network stress testing, new feature testing, GUI and command functionality testing, platform compatibility testing, backward-compatibility testing, and regression testing.

New software version releases are handled through GitHub using Gitian Compilation/Building. While source is generally made available early to allow for compiling by individuals, crosschecked binaries are released by the developers for general installation and use.[9]

[9] M. Cuperman, *Gitian*, Base Zero, https://gitian.org

3 PROOF OF STAKE CONSENSUS

Unlike its predecessors—Bitcoin, Litecoin, and Dash—the PIVX network functions on a **Proof of Stake consensus algorithm**, which was introduced in a paper by Sunny King and Scott Nadal in 2012[10]. 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 consensus[11]. The robustness of the Proof-Of-Stake was further enhanced in a version 3 of the protocol at the end of 2016[12], and most recently, Zerocoin Proof of Stake (zPoS) was implemented by PIVX in 2018.

- *For more on PIVX's zPoS see section 6.*

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.

[10] S. King, S. Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, 2012.
[11] P. Vasin, *BlackCoin's Proof-of-Stake Protocol v2*, https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf
[12] BlackCoin, Security Analysis of Proof-of-Stake Protocol v3.0, https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf

3 PROOF OF STAKE CONSENSUS CONT.

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.

3.1 PIVX PROOF OF STAKE - IDENTITY AND SECURITY

PIVX utilises staking as it's a strongly held position within PIVX that a fair alternative to PoW is necessary for a decentralised currency to be valid, feasible, and welcoming to newcomers. The design of the **PIVX PoS** and **private zPoS** systems are intentionally tailored to mature in such a way that growth of the network and further adoption work in favour of the network, rather than bog it down and focus power on a select group. PIVX transactions will remain expedient, with elastic block sizes coming soon to ensure this—or instant if electing to use SwiftX; they will remain private—only getting even harder to trace as new implementations following zPIV, such asI2P, and dandelion go live; and they will remain decentralised.

- *For more on zPoS see section 6.*

Criticisms towards PoS consensus networks do exist, such as potential double spending, and vulnerabilities to ***long-range*** and ***nothing-at-stake*** attacks. Staking/masternode rewards require 100 consecutive confirms, making them spendable after 101 block confirms; this protects against network dominance via malicious staking involving exponential growth were a vulnerability ever to be found and exploited.

- *For more on nothing at stake see section 3.1 i.*

It was estimated by a PIVX developer that an attacker would need to own 70.7% of staked coins for a 50% chance of ***double spending*** or invalidating a single block—a number practically impossible to acquire.

Another proposed PoS vulnerability is a ***long-range***, or ***history*** attack, wherein early blocks are rewritten, compromising the blockchain. For this reason, checkpoints—blockchain markers set at intervals preventing any alteration/forking prior to them—are used to maintain the valid chain, and help by protecting against ***long-range*** attacks.

A successful PoS attack would greatly de-value the attacker's assets when discovered, whereas a successful PoW attack may cost an attacker only electricity. Also, PIVX staking can be decentralized amongst all of its users and cannot be traced by electricity use, whereas mining is usually centralized by mining cartels, concentrated in regions with cheap electricity, and is traceable by high constant power demand.

- *For more on privacy and security see section 6.1.*

3.1I ADDRESSING NOTHING-AT-STAKE CRITICISM

Nothing-at-stake is a criticism of PoS focused on the fact that PoS is not resource heavy, and therefore by nature promotes malicious forks. The argument proposes that in the event of a fork, as the staker is not tight on processing power or resource to contribute to both the initial chain, and the fork, supporting both will provide maximum rewards, and so is the best course of action.

Rather than provide an abridged version of the important counterargument to this concern within this document, this comprehensive article written by PIVX PoS developer **Presstab** is strongly recommended. It can be found here: https://pivx.org/nothing-considered-a-look-at-nothing-at-stake-vulnerability-for-cryptocurrencies/

3.2 STAKING PIV AND ZPIV

Both PIV and zPIV can be staked on the PIVX network, with the staking of zPIV via zPoS, rewarding users for utilising PIVX privacy features. Staking either PIV or zPIV on the PIVX network requires at least 1 of the smallest unit of either PIV (0.000000001) of zPIV (1) held within, the wallet to be synchronised with the network with block information up to date, and for the wallet to be unlocked for staking.

While staking is active, it doesn't necessarily ensure users will mint new PIV/zPIV right away. As participating in PoS means a node may hash a block to contribute to the blockchain at any point, and depending on the quantity being staked (the more staked, the higher the chance of being selected). For this reason, variance exists in PIVX staking as rewards are not allocated regularly, but are randomly awarded per the hashing competition of the PoS consensus model.

- *For more on staking rewards see section 5.*

A guide for setting up a PIVX wallet for staking can be found here: https://pivx.org/knowledge-base/staking-setup-guide/

4 MASTERNODE NETWORK

The PIVX network is two-tiered. The network is composed of the first, staking tier, in which all PIVX holders can participate in through staking their PIV; and the more exclusive masternode tier.

- *This section is dedicated to the Masternode network. For more on staking see section 4.*

Masternodes are a set of incentivised nodes on a network within the PIVX network responsible for the handling of particular specialised tasks. The PIVX Masternode network has been carried over from Dash, though with the significant restructure to a **Proof of Stake** consensus algorithm. The functions carried out by PIVX masternodes are fundamentally similar, however, to those of Dash. As such, these nodes are an integral part of the PIVX digital ecosystem, and necessary to network functionality.

4.1 MASTERNODE NETWORK TECHNICAL FUNCTIONS

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 one masternode has power or authority in excess of others in the network.

This section dissects these Masternode network functions individually.

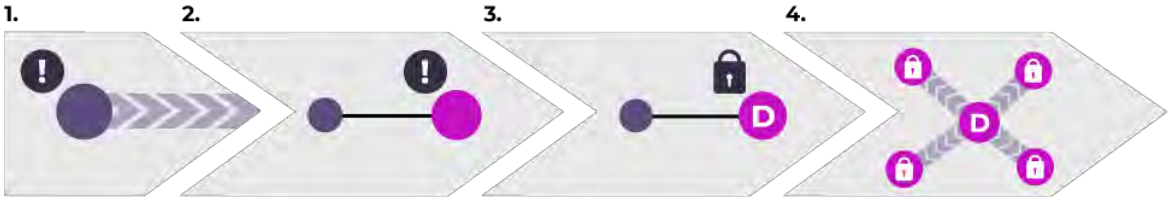
4.1 | SWIFTX

• *The PIVX SwiftX instantaneous transaction logo.*

The Masternode network allows for **near instantaneous transactions, as short as a single second**. With transaction times provided by SwiftX, **PIVX is able to compete with similarly fast crypto currencies**, as well as transactions of credit and bank cards. SwiftX transactions take place independently of the network proper, as they are isolated to the Masternode network.

This function takes place via a quorum between masternodes. When a SwiftX transaction is proposed, the inputs of said transaction are locked by a random delegate masternode, making them spendable only through a specific transaction. All conflicting blocks or transactions would then be rejected. The hash of the locked transaction is broadcast by the delegate via ZeroMQ (a high-performance asynchronous messaging library) over the Masternode network, near-instantly achieving consensus and eliminating the need to await confirmations without the risk of a double-spend.

4.1 | SWIFTX CONT.



• *A basic demonstration of a SwiftX transaction.*

Key: ***Black:*** *standard node.* ***Fuchsia:*** *masternode*

Fuchsia with D*: delegate masternode.* ***!:*** *SwiftX transaction.*

1. *A standard node makes a SwiftX transaction.*

2. *The SwiftX transaction is broadcast to the Masternode network.*

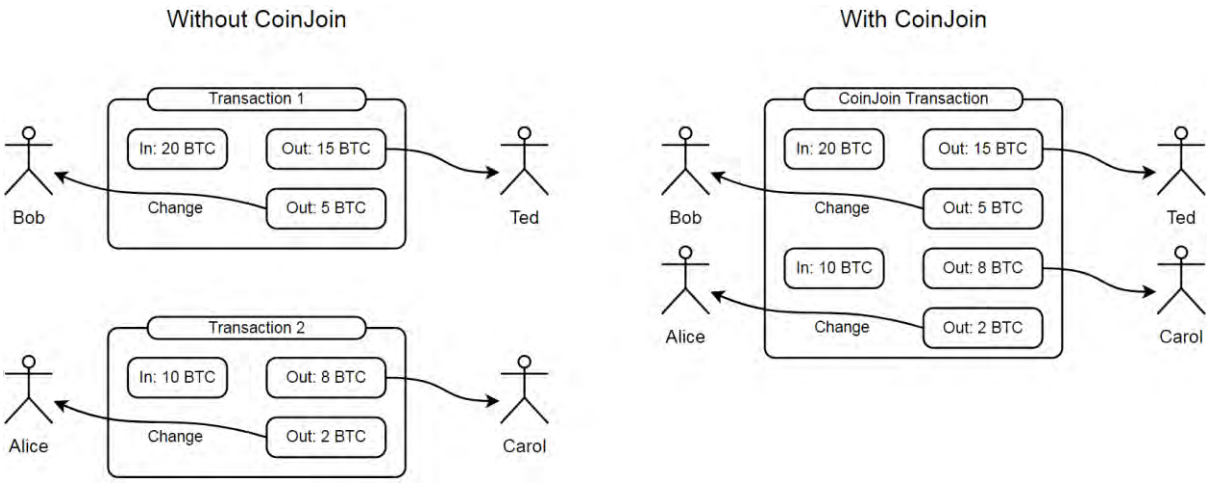
3. *A random masternode becomes SwiftX delegate and locks the transaction.*

4. *The delegate masternode broadcasts the locked transaction to the network, wherein all non-abiding block incidences will be denied.*

The benefit of SwiftX lies in the ability to make transactions as point-of-sale comparable to current systems such as Visa. The difference being that SwiftX is decentralised, with no point of failure.

4.1 II COIN-MIXING

As with Dash's PrivateSend, PIVX's coin-mixing feature was initially built upon CoinJoin. *Coin mixing*—also known as *tumbling*—involves the obscuring of transaction via the dividing of funds to protect their source. Not moving the sum total of a transaction directly from source to target, but rather complicating it via dividing it into mixed transactions, makes it much more difficult to track any one mixed transaction. This process serves to maintain the fungibility of units of the currency.[13]



- *This image*[14] *demonstrates the basic idea behind CoinJoin wherein two transactions are merged into one.*

As PIVX is Proof of Stake, rather than Proof of Work, significant alterations were necessary in order to implement a coin-mixing service optimally into the PIVX code.

Since PIVX Core wallet version 3.0.0 PIVX has moved away from the CoinJoin methodology of coin-mixing, replacing it with ***Zerocoin***—a more sophisticated coin-mixing protocol with heavily improved privacy baked into the cryptography of the protocol. This limits the need for coin-mixing dependency on masternodes. **With Zerocoin in place, PIVX is able to legitimately make private transactions, with no record stored on the blockchain**.

[13] *op cit*. Dash Whitepaper, Section 3.
[14] Image sourced from *Wikipedia*, *CoinJoin*, https://en.wikipedia.org/wiki/CoinJoin

4.1 II COIN-MIXING CONT.

• *The Zerocoin logo.*

Zerocoin newly mints currency (**zPIV**) and allocates it to pools in order to draw from when a wallet receives zPIV. These pools represent a substantial amount of the total PIV, at the time of writing this document, the number exceeds 20%. Thus, with zPIV there is no necessity to obscure a coin's origin, as **zPIV carry no data pertinent to a unit's history, maintaining fungibility while being untraceable**.

PIVX will continue pioneering new technology to remain at the very forefront of privacy in the crypto sphere. The next frontier for PIVX in this space is the addition of *Bulletproofs* and the replacement of the RSA-2048 Factor system currently in place with a more modern solution.

- *For more on the PIVX Zerocoin protocol, Bulletproofs, and zPIV see section 6.*

4.2 MASTERNODE DECENTRALISED GOVERNANCE

As a ***Decentralised Autonomous Organisation*** (DAO), PIVX operates and abides by its own community self-governance. No one 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.

The means through which this form of governance is currently achieved is through the Masternode network. 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 1000 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.

- *For more on masternode acquisition see section 4.3.*

While masternode operators currently hold the exclusive right to vote on proposals, this does not exclude other members of the PIVX community from impacting upon the future of PIVX. Anyone has the ability to make a proposal for consideration. Channels of communication exist through which all community members are welcome to take part in discussions on current proposals, as well as the reconsideration of existing projects passed in previous votes. In this way, by participating in discussions and offering input, all members of the PIVX community have a say, even if they are unable to cast a vote.

While this system highly disperses power, it's worth noting that when put to vote recently, the PIVX community voted in favour of further distributing power through the community. As such, it is a high priority goal in 2018 to settle on a form of ***Community Designed Governance***—a governance designed by and for the community that all members of the community can agree is in everyone's best interest.

- *Community Designed Governance is currently in the process of being realised. For news on PIVX's Community Designed Governance as it becomes available, watch:* https://pivx.org/what-is-pivx/roadmap/.

4.2 | PROPOSAL VOTING

Currently, the Masternode network is responsible for voting on proposals that collectively determine the direction PIVX moves in. Each masternode in the network is entitled to one vote on any given proposal, and a majority will determine whether or not a proposal is passed.

The masternode network offers a decentralised voting mechanism set up in the rules governing the blockchain. This allows PIVX—among other things—to hire core developers and pay them directly after approval of the work in a decentralised fashion.

A masternode is able to vote on a proposal using commands inside the wallet, or tools outside of it. The vote then propagates across the network and is validated and recorded as a blockchain object.

As current governance operations function, the ability to vote is restricted to those operators of masternodes. This is, however, subject to change in the future.

- *For more on PIVX governance see section 4.2.*

The current voting system functions by having a proposal voted on the Masternode network, however, reaching the voting stage is not the beginning of a proposal's lifecycle. As a general rule, proposals have a lifecycle as follows:

Community discussion takes place—usually via **PIVX Discord** (discord.pivx.org). Here a proposal is introduced to active members of the PIVX community, with the general details being discussed, and members giving input based on initial impressions.

A forum post is made—forum.pivx.org - Budget & Governance Proposals –> **Pre-Proposal Discussions**. Here an idea is expressed in more concrete terms, and properly vetted by the community. Unlike the ephemeral nature of a live chat, forum posts last long enough to be seen by more eyes, as well as carefully considered. In this stage, a proposal should consolidate, being added to and altered in accordance with critique and unforeseen challenges that must be pre-emptively addressed. To maximise the benefits of this stage, as much attention should be drawn to the proposal as possible, and as such various channels of communication should be used to the benefit of the proposal.

An official proposal, now matured with its mettle tested and concerns addressed by forum discussion, is added to the forum as a proposal post— forum.pivx.org - **Budget & Governance Proposals**. This is paired with a proposal added to the blockchain—which must be made more than **72 hours** from the next *superblock*—in order for masternode holders to vote on. An initial fee of **50 PIV** is paid by the proposer to submit a proposal for consideration. This fee can be **reimbursed** if so requested as part of the proposal, but must be paid regardless of the proposal passing or not.

- *A detailed explanation on how to submit a proposal can be found here:*

https://pivx.org/proposals/

technical details here:

https://forum.pivx.org/t/howto-create-a-proposal/959

Proposals are voted on by the Masternode network. For a proposal to pass, 50% of active voters must submit a vote on the proposal. From this, yes votes minus no votes must exceed 10% of total masternodes in order for the proposal to pass. In the event a proposal is passed, an additional fee of **5 PIV** is required in order to implement the proposal. This fee, too, can be **reimbursed** if such an action is included in the proposal outline. From approximately **48 hours** (2880 blocks) out from the superblock, votes will be finalised at a random time, ensuring no last minute manipulating can occur.

Implementation comes with the next superblock, and the proposal becomes part of PIVX, with the funds for the budget that had been burnt on a per-block basis through the most recent cycle being afforded to the superblock total budget.

Again, note that this procedure is subject to change with the inevitable reformation of PIVX to further decentralised as it moves towards its goal of utilising PIVX's ***Community Designed Governance***. Nevertheless, it's highly likely the general procedure will remain largely intact, with the primary change being to who has the ability to cast votes.

4.3 MASTERNODE ACQUISITION

Operating a masternode on the PIVX Masternode network is an attractive option to those invested in PIVX. Masternodes are incentivised, paying out PIV to the operator in return for their service. Masternodes are run via the standard PIVX wallet, albeit with some additional input.

To be eligible to create a masternode, several requirements must be fulfilled. A masternode necessitates the following:

10,000 PIV be stored on the masternode controlling wallet. These PIV must remain unspent so long as they are associated with a masternode wallet—this should be a separate wallet from one used to make transactions. Spending, or otherwise removing these PIV will remove the status of the host wallet as a masternode, taking with it the eligibility for masternode rewards. The necessity of these 10,000 PIV serves several purposes, including ensuring a high enough percentage of nodes remain staking, and that the masternode host is likely to reliably provide a masternode service for the network over time, rather than simply dabbling. Most importantly though, it ensures no single entity can simply host enough masternodes to achieve the 51% necessary to corrupt the governance, jeopardising the PIVX DAO.

An unchanging static IP is also necessary to operate a masternode. Dynamic IPs cannot participate in the network as consistent contact with a verified masternode is necessary to function in the Masternode network. This means the internet connection of the masternode host must also be reliable, as the masternode needs to remain online dependably. On top of this, each masternode requires a unique IP, so hosting two masternodes cannot be accomplished without a secondary IP address. In the event this requirement is not possible, it is recommended the user simply stakes their PIV instead. This pays out a similar amount to a masternode, though downtime in connectivity is harmless if encountered.

- *For more on staking see section 3.*

A degree of technical competency is also preferable, as although resources are available for the setting up of a masternode, the process requires editing of a *.conf* file, allocation of a new wallet address, and other actions executed by Linux command console. Support for setting up a masternode can be gained through PIVX support channels.

- *Instructions on setting up a masternode can be found here:*

  https://pivxmasternode.org/category/masternodes/ *with sections containing links to the most up to date data.*
- *PIVX support can be reached on the PIVX Discord in the #support channel, or at https://pivx.org/support/*

4.3 MASTERNODE ACQUISITION CONT.

Masternodes can be run on Linux machines, through a server host, or through devices such as the Raspberry Pi. Ultimately, despite the decision, the security of the masternode host is integral. Private key management, the setting up of a firewall, a physically protected machine, and other security measures are **strongly** advocated for, both for the sake of the network, and the 10,000 PIV of the host.

As with anything PIVX, there is no need to go it alone when setting up a masternode. Support can always be found from the PIVX community. Any questions can be posed to the community in the Discord server (**discord.pivx.org**).

5 MASTERNODE - STAKING REWARD SYSTEM

As a two-tiered network, PIVX incentivises participants of both the staking and Masternode tiers to maintain the health of the network. Via PoS, users contributing towards the network are rewarded either for staking in-wallet, or for storing their 10,000 PIV as collateral for a masternode to support the network. While both of these are a means of acquiring rewards over time, the amount and means differs.

- *For more on masternodes see section 4.*

5.1 REWARD BALANCE: MASTERNODE - STAKING

The reward balance between a masternode and a staking wallet is overall not significantly skewed. Generally, the masternode will pay out reliably, where staking involves more variance. This reliability is to incentivise masternodes, as they are integral for the health of the network.

A masternode has several qualities that set it apart from a staking wallet:

- It requires 10,000 PIV be left unusable by the holder to remain functioning as a masternode.

- It must be left connected at all times.

- It requires a separate, stable IP address to the user's wallet intended for use.

* **Note** Some aspects of the setting up of a masternode can be complicated for less technically-minded users.

These lack of freedoms mean that if the reward were to be identical to staking, the likelihood of anyone choosing to host a masternode would be significantly lower.

With that said, there are advantages to staking over hosting a masternode. These include:

- The ability to opt in and out of staking as the user pleases.

- Can be done regardless of held PIV/zPIV amount.

- The option to divide up holdings between addresses.

- No requirements on specific denomination (masternode 10,000 requirement).

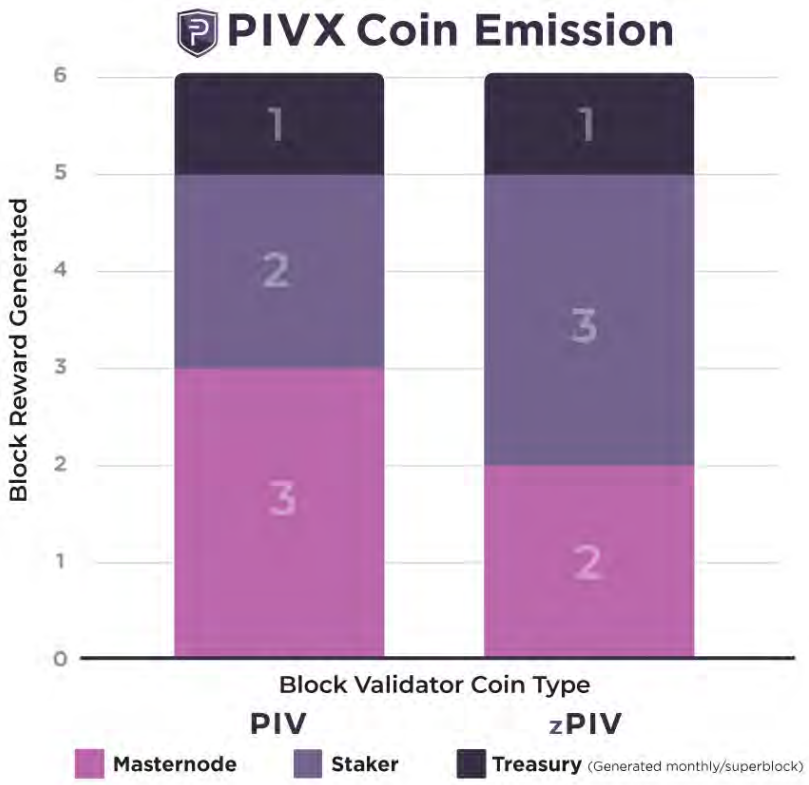
5.1 REWARD BALANCE CONT.

There also exists the possibility to earn more than a masternode holding the same amount of PIV due to the random nature of staking. On the flipside, this may also mean one is rewarded less than the average expected amount for staking at the held amount.

At the same time, zPIV offer an increased incentive for stakers over PIV. Here is a breakdown of the minted currency in the event of PIV and zPIV staking node respectively:

PIV staker finds block: 3 PIV to masternodes, 2 PIV to staker, 1 PIV budget

zPIV staker finds block: 2 PIV to masternodes, 3 zPIV to staker, 1 PIV budget



In the case of zPIV, masternodes are less favoured than stakers. Compensation for this exists in frequency and through zDEX fees being paid out to them when facilitating transactions through zDEX.

- *For more on zDEX see 6.4.*

Note PIVX utilised a seesaw system to balance staking-masternode rewards in the past, but Zerocoin and new features have complicated the process, necessitating the new system outlined above.

5.2 REWARD RATE VARIANCE: PIV - ZPIV

As seen in the previous section, PIVX and zPIV rewards differ in both staking and masternode rewards. This discrepancy is part of an incentive to have users in the PIVX network support Zerocoin, which by nature cannot function without participation. Liquidity of zPIV over the Zerocoin protocol is also necessary for it to function swiftly. Non-locked volumes of zPIV need to be available for the protocol to draw on at all times, lest transaction time become needlessly extended. This is due to the wait on both transaction confirmations, and a confirmation of another zPIV mint of the same denomination to meet the maturity requirement—non-issues providing the zPIV liquidity is supported.

These mechanics of Zerocoin are explained in more detail in section 6, though the variance in rewards between PIV and zPIV is a necessity for the health of the PIVX network. Careful consideration has been invested into fairly balancing the rewards for both PIV and zPIV, but as privacy and expediency are the ultimate goals of PIVX, the health of the Zerocoin network is paramount.

- *For more on Zerocoin and zPIV see 6.*

6 ZPOS - PRIVATE POS THROUGH THE ZEROCOIN PROTOCOL

- *The logo and name of the Zerocoin protocol on PIVX purple.*

The addition of the Zerocoin protocol to PIVX has been instrumental in establishing truly private transactions and holdings in PIVX. Zerocoin was initially taken from the proof of concept libZerocoin library, which became abandonware once its creators moved on from the project. Freely useable and open source, the PIVX team turned *libZerocoin* into the PIVX Zerocoin protocol, and with it, the accompanying zPIV.

- *For more on libZerocoin see section 2.5.*

The challenge of implementing Zerocoin into PIVX was that it was initially designed for use with Bitcoin, a PoW oriented system.[15] PIVX, however, function through PoS consensus, which made necessary substantial alterations to the Zerocoin base, available as *libZerocoin*. The result of this customisation of Zerocoin is the PIVX Zerocoin PoS protocol, **ZPoS**.

[15] *op. cit., Zerocoin: Anonymous Distributed E-Cash from Bitcoin*

6 ZPOS - PRIVATE POS THROUGH THE ZEROCOIN PROTOCOL CONT.

zPoS is PIVX's **private** Proof of Stake protocol based on **Zerocoin**. Unlike most other Proof of Stake cryptocurrencies, zPoS allows users to **remain anonymous while staking** their zPIV and earning rewards for doing so.

Users are incentivised to use zPoS by a 50% increase in staking rewards. This incentive ensures sufficient users participate in zPoS, maximising **privacy** and **security** by protecting against potential timing attacks or other malicious, invasive actions. In this way, it is the aim of PIVX to have users primarily utilising the zPoS system, with PIV as an alternative for those requiring the full transparency and disclosure of the blockchain.

- *For more on security see sections 3.1 and 6.1 ii.*

Staking of zPIV requires no special requirements beyond using a version of the PIVX Core wallet beyond 3.1. Users can stake zPIV providing they meet the minimum requirement of holding sufficient funds to mint one zPIV, as smaller denominations of zPIV are unavailable at this time.

- *For more on staking and staking rewards see sections 3 and 5 respectively.*

6.1 ZEROCOIN PROTOCOL ANONYMITY

The Zerocoin protocol provides anonymity on transactions through a protocol-level coin mixing service. It uses zero knowledge proofs—sending no information between sender and receiver—establishing pools for *zPIV* in accumulators which are drawn from in order to pay out transactions with zPIV coins that carry no data pertinent to their history. zPIV can be minted from PIV at user discretion for a small fee, destroying the PIV converted to zPIV.

- *For more on zPIV see section 6.2.*

Zero-knowledge as a concept has been demonstrated through the following example:

Imagine your friend is colour-blind and you have two balls: one red and one green, but otherwise identical. To your friend they seem completely identical and he is skeptical that they are actually distinguishable. You want to prove to him they are in fact differently-coloured, but nothing else, thus you do not reveal which one is the red and which is the green. Here is the proof system. You give the two balls to your friend and he puts them behind his back. Next, he takes one of the balls and brings it out from behind his back and displays it. This ball is then placed behind his back again and then he chooses to reveal just one of the two balls, switching to the other ball with probability 50%.

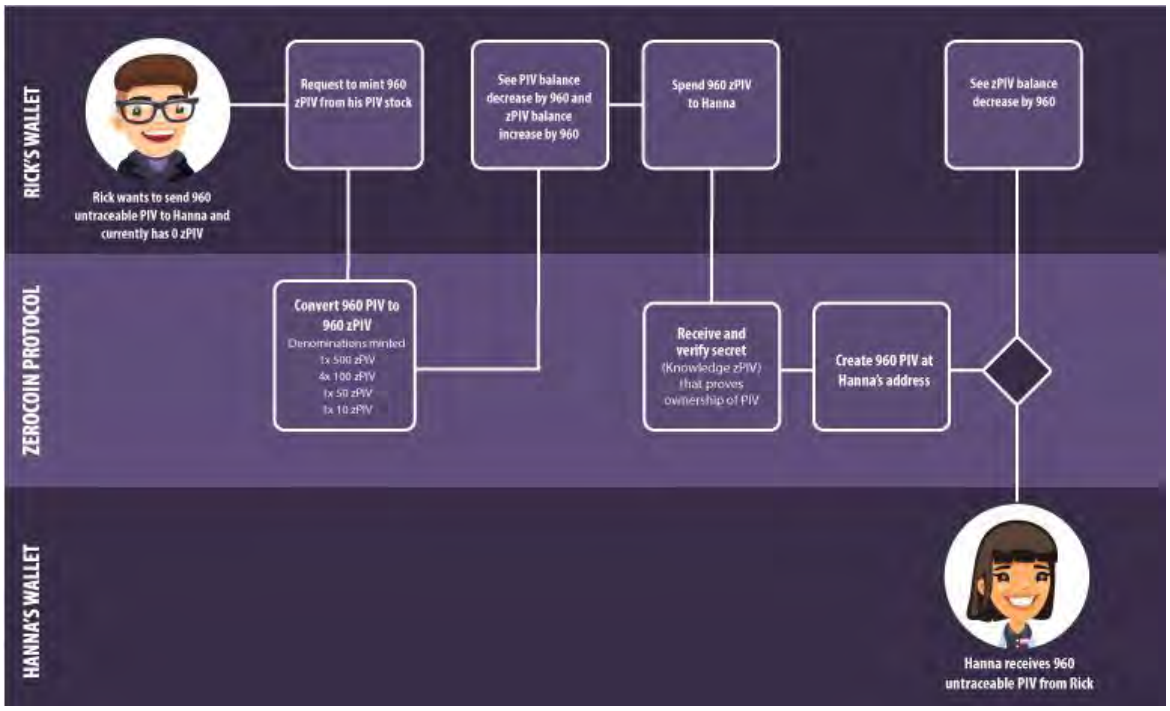
He will ask you, "Did I switch the ball?" This whole procedure is then repeated as often as necessary. By looking at their colours, you can of course say with certainty whether or not he switched them. On the other hand, if they were the same colour and hence indistinguishable, there is no way you could guess correctly with probability higher than 50%. If you and your friend repeat this "proof" multiple times (e.g. 128), your friend should become convinced ("completeness") that the balls are indeed differently coloured; otherwise, the probability that you would have randomly succeeded at identifying all the switch/non-switches is close to zero ("soundness"). The above proof is zero-knowledge because your friend never learns which ball is green and which is red; indeed, he gains no knowledge about how to distinguish the balls.[16]

See *https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff* for an alternate explanation.

[16] Taken from Wikipedia, *Zero-knowledge proofs*, https://en.wikipedia.org/wiki/Zero-knowledge_proof#Abstract_examples

6.1 ZEROCOIN PROTOCOL ANONYMITY CONT.

The use of the Zerocoin protocol replaces that of the coin mixing method, CoinJoin, formerly employed by standard PIV transactions prior to the introduction of Zerocoin in PIVX Core wallet 3.0.0, as Zerocoin is in all ways a further advanced means of performing anonymous transactions.



- *Original image concept by mcl4m.*

The above image demonstrates in simple terms how a Zerocoin transaction occurs. It traces the minting of Bob's zPIV from PIV, with the total 960 zPIV sum being made up of denominations in which zPIV can be used. These denominations are pooled, with none of the newly minted zPIV being traceable back to Bob's initial PIV. Bob's new zPIV, now linked back to him only in ownership, can be sent to Amanda without any link existing tying Bob, Amanda, and the transaction together. It's always good practise to mint zPIV well ahead of a spend to further increase factors complicating tracing any particular spend to a source.

It's worth noting that this particular transaction example uses four different denominations of zPIV in order to make up the total of 960 zPIV. In order to spend zPIV, at least one zPIV minting of your denomination must first be made. This maturity measure is in place to ensure privacy, as there may be the potential, no matter how small, to trace back transactions if at any point only one sender utilises a particular denomination. For this reason, the reward system incentivises the staking of zPIV higher than it does PIV in order to keep the accumulators stocked, and zPIV being minted.

6.1 ZEROCOIN PROTOCOL ANONYMITY CONT.

PIVX *Zerocoin protocol* Technical Specs (v2.0)

Key Features: Custom accumulator checkpointing system

zPIV version 1 Phase Period: October 16th 2017 to March 29th 2018 (FINISHED)

zPIV version 2 Phase Period: May 01th 2018 onward (CURRENT)

zPoS Phase Period: May 08th 2018 onward (CURRENT)

Accumulator Modulus: RSA-2048

zPIV Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000

Mint time: >= 0.5 seconds

Spend time: >= 2.5 seconds

Maximum single Spend limit: 35,000 PIV

Maximum single Spend denomination count limit: 7

Block size: 2 MB (was 1 MB before v3.0.0 zPIV wallet)

Fees (mint): 0.01 PIV per minted zPIV denomination.

Fees (spend): No fee to spend zPIV back to PIV.

Minimum PIV confirmation count required to mint zPIV: 6

Minimum zPIV confirmation count required before spend: 20

Maturity requirement before zPIV can be spent: 1 new identical denomination mint added to accumulator after yours is added.

Confirms before zPIV can be staked again: 200.

- *For more on PIVX coin specs see section 2.1.*
- *For more on Bulletproofs see section 6.1 i.*

6.11 ZEROCOIN BULLETPROOF AND SETUP TRUST

A known concern sometimes voiced with zero knowledge proofs is in the reliance on a fully *trusted* setup system. In a space where *trustlessness* is a highly sought after goal, this reliance is often seen as less than ideal.

Despite there being no practical weakness or exploitation in current trusted zero knowledge systems, work is underway to shift to a trustless setup in the future. At this point, work is heavily theoretical, and a number of potential solutions are being vetted. Further information will be made available in the future.

PIVX is also in the process of integrating a customized implementation of the Bulletproofs paper to lower the communication costs of the Serial Number Signature of Knowledge (the essential part of a Zerocoin spend).

Bulletproofs were developed as a joint venture between Stanford University, University College London, and Blockstream. Bulletproofs are described as:

> "...short non-interactive zero-knowledge proofs that require no trusted setup […] Bulletproofs are designed to enable efficient confidential transactions in Bitcoin and other cryptocurrencies. Every confidential transaction contains a cryptographic proof that the transaction is valid. Bulletproofs shrink the size of the cryptographic proof from over 10kB to less than 1kB."[17]

The change to Bulletproofs will provide a significant reduction in Zerocoin spend size, further optimising the blockchain for Zerocoin spends.

Ongoing efforts are geared towards laying the groundwork for the progressive Bulletproofs integration. The current protocol is being rephrased into arithmetic circuits—a method for describing problems from complexity theory. Cryptographic literature provides many zero-knowledge arguments for proving the knowledge of a solution to an arithmetic circuit very efficiently.

Work towards implementing lowered proof size is progressing nicely, as recent work has seen the signature of knowledge lowered from up to 20Kb to under 5Kb, for a total spend size of around 11k when including the proof of accumulation and overhead. Further lowering the size of spends is goal moving forward.

[17] *Bulletproofs: Short Proofs for Confidential Transactions and More*, https://crypto.stanford.edu/bulletproofs/

6.1 ZEROCOIN BULLETPROOF TRUSTLESSNESS CONT.

The implementation of Bulletproofs is based upon cryptography from well respected security conferences, and is being reworked to suit PIVX's use case scenario. While the proof of concept exists, the development and integration is something that needs to be handled carefully, and with utmost respect for the integrity of the final product.

To learn more about Bulletproofs, the research paper on the emergent protocol can be found at the following web address:
https://eprint.iacr.org/2017/1066.pdf

6.1II ZEROCOIN, PRIVACY, AND SECURITY

With Zerocoin, as a **PoS network**, the PIVX Masternode network is inherently more resilient to such vulnerabilities as *Sybil attacks*, as no PoW mining can be monopolised and taken advantage of. The lack of ability to self-spend to produce a malicious honeypot highly resists such an attack. As such, setting up a Sybil attack would be more costly than simply purchasing sufficient funds to control a majority of masternodes, each requiring 10,000 PIV, and unique IP addresses. As the number of masternodes currently exceeds 1,300, a 51% attack like this would require an unrealistic amount of money once supply and demand are factored in. Further, with changes to the voting system, and other measures in development, attacks such as these become even less practical.

- *For additional notes on PIVX PoS security see section 3.1.*

Zerocoin mints produce **newly minted zPIV** to be held in separate accumulators, and Zerocoin spends are converted to **newly minted PIV** on arrival ensure no transaction has a traceable history so long as Zerocoin is utilised. Unlike other privacy coins, **PIVX privacy is not a secret hidden on the blockchain waiting to be deciphered**, but a product of complete severance from prior transactions. **Maturation** requirements and **higher zPoS rewards** also ensure the pools from which zPIV are drawn are always vast enough that tracing address spends by narrowing in is a statistical impossibility.

Soon, new features will improve upon the privacy and security of Zerocoin and PIVX, with permissioned staking, the dandelion protocol, I2P, U2F, and other implementations that will only further make PIVX one of, if not the most private and secure cryptocurrency available, protecting the users, transactions, and origins thereof.

6.2 zPIV

zPIV are the coin used by PIVX's Zerocoin protocol. They are **NOT** a unique cryptocurrency from PIV, but rather a form taken by PIV when allocated Zerocoin status. As such, the **value of zPIV is identical to that of PIV**, and the two can be freely switched between within the PIVX wallet.

While zPIV are not disparate from PIV, they are listed as a separate balance within the wallet. The sum of both PIV and zPIV is calculated providing the total balance displayed within the wallet.

zPIV are newly minted when PIV are allocated Zerocoin status by user input via the wallet. The minted zPIV will replace the value of PIV removed from the network. In this way, zPIV are free of a history on the blockchain, meaning they cannot be traced back to any user through a transaction history, yet the economy remains stable. This also applies to the PIV received via zPIV transaction, which, too, will be newly minted.

zPIV exist within the accumulators in denominations of **1**, **5**, **10, 50**, **100**, **500**, **1000**, and **5000**. Denominations smaller than these are a potentiality, though currently are not necessary as judged by volume and PIVX's value.

When spending zPIV, if the transaction is of an amount the denominations of zPIV cannot cover, the nearest value is given, with the difference being made up in PIV returned as change to the sender. Due to this, although it is more convenient to spend zPIV using combinations of these denominations, it is not a necessity.

To prevent spam transactions, or more malicious attacks, **zPIV minting incurs a small fee** (0.01 PIV per denomination), which is burnt to maintain the health of the PIVX economy. As zPIV denominations currently are set at **1**, **5**, **10, 50**, **100**, **500**, **1000**, and **5000**, if a user chooses to mint, for example, 18 zPIV, the fee incurred would be 0.05 PIV, as the sum would be comprised of a 10, 5, and three 1 zPIV denominations, for a total of five times 0.01 on each amounting to 0.05 PIV.

6.2 ZPIV CONT.

Ultimately, it is the goal of PIVX to have the majority of business on the PIVX network be conducted with zPIV. This is not to say PIV will be phased out, however, as the option to use PIV will remain for such use cases as the highest possible transaction speeds using SwiftX for retail purposes.

Every minted zPIV denomination made **before** the release of **deterministic zPIV** is associated with a unique serial number that is stored in the local **wallet.dat** and not on the blockchain. This means that zPIV denominations minted in older wallet versions should be backed up via wallet.dat as the previous backup will not have the serial numbers for the newly minted zPIV denominations. As the network no longer supports older instances of the Core wallet, this should be a non-issue outside of those loading outdated wallets.

Deterministic zPIV are generated using a unique 256 bit seed generated on a wallet's first run. The deterministic seed is used to generate a string of zPIV that can be recalculated at any time using the seed. Deterministic zPIV allows for users to backup all of their future zPIV by recording their seed. The zPIV seed is needed by the wallet to spend the zPIV after it is generated; if the seed is changed then the coins will not be spendable as the wallet cannot regenerate the private zPIV data without the seed. It is important that users record their seed after their first run of the wallet. If the wallet is locked during the first run, then the seed will be generated the first time the wallet is unlocked.

The addition of deterministic zPIV adds encryption to what would otherwise be unencrypted, raw Zerocoins. It's important, however, to keep the dzPIV seed safe, as it serves as a key to your held zPIV should it be compromised, much in the way the wallet's private key does.

The serial number and other essential zPIV data are committed to the database (wallet.dat) before the transaction is completed and broadcasted to the network. This minimizes the risk of losing your freshly minted zPIV denominations during an unexpected event during the minting of zPIV, such as a PC crash or internet connectivity issues.

In August of 2018, PIVX achieved the first Zerocoin mint and spend on an Android-based, light-node (doesn't store the entire chain) using a custom protocol.

6.3 MINTING AND STAKING ZPIV V2 FOR ZPOS

With the onset of **PIVX Core wallet version 3.1.0**, **zPoS** was introduced to PIVX, allowing users to **stake zPIV** as they have previously been able to do PIV. As with PIV, staking zPIV earns rewards randomly dependent on held funds, though the **reward is higher for the staking of zPIV—3**, rather than the **2** of PIV. It's important to note that zPIV minted **prior** to the release of version 3.1.0 and are **not eligible** for staking, as zPIV minted following the release are designated as zPIV v2, and only these are compatible with zPoS.

In the event a user wishes to stake their zPIV minted with an earlier wallet version, they are required to **convert** their zPIV to zPIV v2. This can be achieved by sending the zPIV to their own receiving address, and subsequently re-minting.

Staking of zPIV requires no special requirements beyond ensuring they are zPoS compatible.

- *For more on staking and staking rewards see sections 3 and 5 respectively.*

6.3 MINTING AND STAKING ZPIV V2 FOR ZPOS CONT.

Following are additional notes on zPIV v.2

Version 2 Zerocoins

Several critical security flaws in the Zerocoin protocol and PIVX's Zerocoin implementation have been patched. Enough has changed that new Zerocoins are distinct from old Zerocoins, and have been labeled as version 2. When using the zPIV Control dialog in the QT wallet, a user is able to see zPIV marked as version 1 or 2.

zPoS (zPIV staking)

Once a zPIV has over 200 confirmations it becomes available to stake. Staking zPIV will consume the exact Zerocoin that is staked and replace it with a freshly minted Zerocoin of the same denomination as well as a reward of three 1 denomination zPIV. So for example if a 1,000 zPIV denomination is staked, the protocol replaces that with a fresh 1,000 denomination and three1 denomination zPIVs.

Secure Spending

Version 1 Zerocoins, as implemented by Miers et. al, allow for something we describe as serial trolling. Spending Zerocoins requires that the spender reveal their serial number associated with the Zerocoin, and in turn that serial number is used to check for double spending. There is a fringe situation (which is very unlikely to happen within PIVX's Zerocoin implementation due to delayed coin accumulation) where the spender sends the spending transaction, but the transaction does not immediately make it into the blockchain and remains in the mempool for a long enough duration that a troll has enough time to see the spender's serial number, mint a new Zerocoin with the same serial number, and spend the new Zerocoin before the original spender's transaction becomes confirmed. If the timing of this fringe situation worked, then the original spender's coin would be seen as invalid because the troll was able to have the serial recorded into the blockchain first, thus making the original spender's serial appear as a double spend.

The serial troll situation is mitigated in version 2 by requiring that the serial number be a hash of a public key. The spend requires an additional signature signed by the private key associated with the public key hash matching the serial number. This work around was conceived by Tim Ruffing, a cryptographer that has studied the Zerocoin protocol and done consulting work for the ZCoin project.