PIVX Zerocoin (zPIV) Technical Paper

Revision 0.9
Last updated October 16 2017

PIVX OVERVIEW

PIVX is a Bitcoin-based community-centric cryptocurrency with a focus on decentralization, privacy, and real-world use. It utilizes an energy efficient Proof of Stake protocol and a second-tier Masternode network for inclusive community-based governance along with a blockchain based self-funding treasury system ensuring its sustainability.

PIVX is continuously striving to achieve a better governance system, instantaneous private transactions, and fungibility in order to remain next generation cryptocurrency.

In layman's term, PIVX is basically a form of online digital money that can be easily transferred all around the world in a blink of an eye with nearly non-existent transaction fees. You can convert your money into PIVX at various exchanges and just hold to earn rewards similar to interest, trade on an exchange to buy other digital currencies or buy goods or services online and offline where it is accepted.

It is not owned or governed by any single person or organization and its network is secured by thousands of nodes all around the world by its users.

The goal of PIVX is to be an advanced digital currency that is fast, secure, decentralized & private.

CRYPTOCURRENCY TRANSACTION PRIVACY

Most common cryptocurrencies such as Bitcoin has a well known public ledger system where all transactions are visible and traceable through its block explorer. This results in anyone and everyone having the ability to see all associated transactions and balances but more importantly its associated addresses as well. This means that the history of its previous address owner is now visible through your own address once the coins have traversed through the blockchain and end up in your own wallet address.

An address may seem like it is fully anonymous but if you made a transaction with an address that is generated by the exchanges and/or other merchant services, you have essentially linked your anonymous address with an address that may lead to your identity.

In most scenarios, such transparency may not be an issue. But it could become a serious problem if the coin that you hold was once associated with an undesirable history or if your address was being targeted by potential thieves.

For example, coin you received was from an address owned by a person or organization that has been conducting illegal activities and was being monitored and tracked by governing authorities. This now means that you may be questioned on your relationship to the previous owner of those coins that you now possess even though you received them legitimately and without knowledge. This could also mean that the coins with such history may be deemed less valuable than those coins without resulting in reduced fungibility.

OUR SOLUTION = ZEROCOIN PROTOCOL (zPIV)

To overcome this issue, beginning with the v3.0.0 core wallet update released on October 7th 2017, PIVX has implemented a well known highly-vetted protocol called Zerocoin with many custom enhancements allowing blockchain-level transaction anonymity in the way of unlinkability.

We call this **zPIV**, where PIV is a unit of PIVX and z prefix is for Zerocoin.

What zPIV provides is a protocol-level coin mixing service using zero knowledge proofs to sever the link between the sender and the receiver with 100% anonymity and untraceability. This means that each coin that gets sent using zPIV is now 100% fungible as it has no determinable history attached to them.

The use of zPIV also means your balance can be masked to avoid being targeted by potential thieves. This is a very unique feature that nearly no other cryptocurrency currently in the market possesses.

PIVX zPIV accumulators are encrypted using RSA-2048[1] challenge generated keys which negates the need for a developer trusted setup and means that no individual knows the factors. This means that everyone's privacy is ensured through the use of zPIV.

UNIQUE FACTOR

As of writing (SEP 2017) PIVX is the *only* Proof of Stake cryptocurrency to have implemented the full set of Zerocoin protocol ideologies and practices. While based on the original libzerocoin public repository that was created by academic cryptographers, the majority of the PIVX zPIV code is custom, making zPIV very unique also.

Original Zerocoin Whitepaper: https://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

Unlike most other cryptocurrencies that currently utilize a zerocoin-based protocol, PIVX zPIV utilizes a very efficient accumulator checkpointing system which allows the zPiv spend process to utilize checkpoints that contains all mints that were made prior to the zPiv mint being spent, as well as a user selected amount of zPiv mints beyond the checkpoint. This allows for a large pool of coins in the accumulator while still having much smaller computation requirements. PIVX's zPiv implementation yields minimal resource consumption and makes zPIV transactions one of the fastest private transfers in the market today.

PIVX zPIV TECHNICAL ADVANTAGES

1. Smaller spend transaction sizes by an average of 25% over any other current implementation in a production environment (further optimization in the works)
2. Fast verification and network sync performance
3. Direct spend of zPIV to a PIVX address
4. Multiple Zerocoin denomination spends is possible in a single transaction
5. Ability to spend exact amounts and issue the remaining change to either a PIVX address or more zPiv.

REAL LIFE BENEFITS OF USING zPIV

1. zPIV can hide your coin balance from prying eyes protecting you from being targeted.
   - So your zPIV balance isn't linked to any particular address.
2. zPIV can hide the transaction history of the coins being sent.
   - Source & target addresses aren't visible making it private, safe & fungible.
3. zPIV anonymous transactions are very fast.
   - It takes as little as 0.5 seconds to mint and 2.5 seconds to spend zPIV.
4. Automatic conversion to zPIV is enabled by default but transparent transfer option is still available.
   - It means that you can always send a fully transparent transaction when required.

HOW ANONYMITY IS ACHIEVED

1. Mint (convert) your PIV into zPIV denominations. (Wallet auto-mints some by default)
2. Spend (send) your zPIV as PIV to any internal or external PIVX wallet address

Essentially the zerocoin protoco pools (thus combines) all the zPIV that people have converted (minted) from their PIV balance into set denominations and uses them to send when a spend is initiated. Keep in mind that the pooling does not mean that everyone's zPIV is stored in a centralized location. Rather, the public ledger (decentralized blockchain) keeps track of how many zPIVs are created.

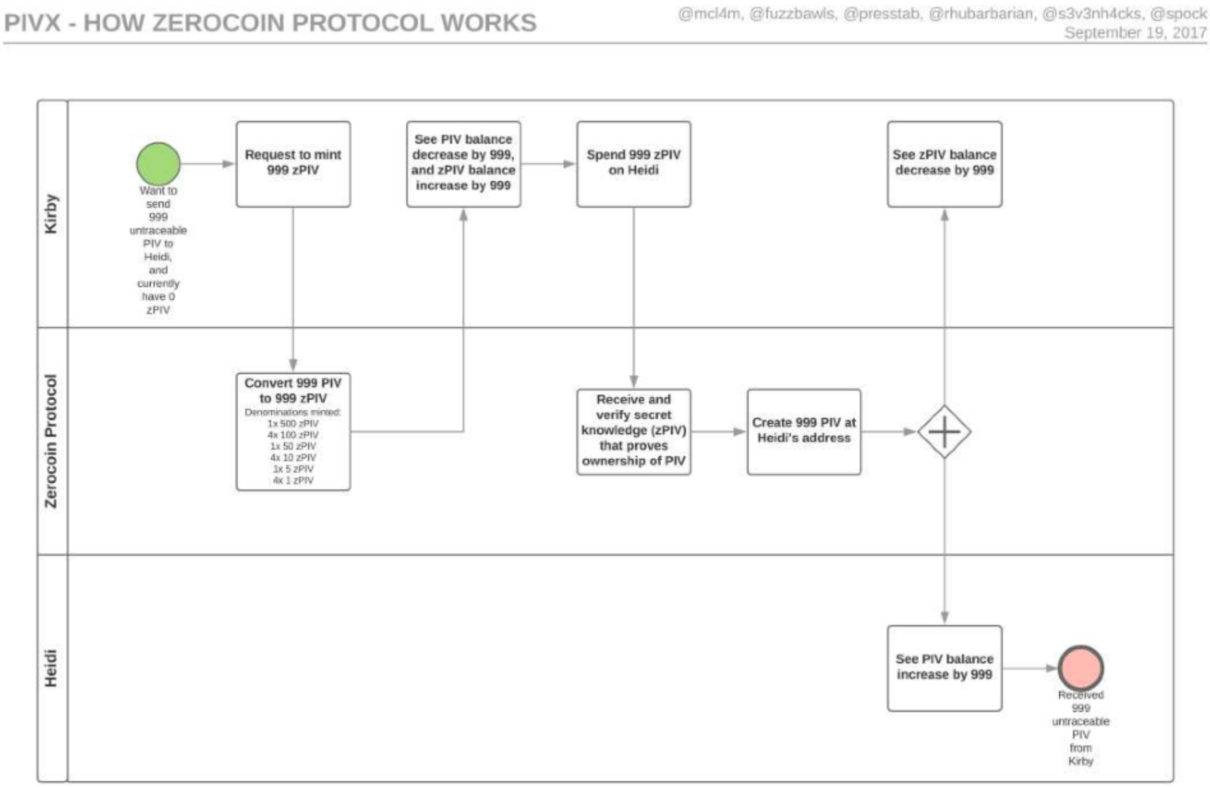
When you want to send (spent) some zPIV amount to a PIVX address, your wallet sends a zero-knowledge proof to the blockchain that allows the zPIV to be converted back to PIV and sent to the target address all in a single step.

Since zPiv spending creates brand new coins if a spender can provide zero-knowledge proof that she has coins in the accumulated pool (accumulator), the coin's transaction history from its previously associated addresses become unlinked and thus results in an untraceable transaction.

Finally, a simple analogy. Think of zPIV as casino chips. You give your 100 dollar bill (i.e. PIV) to the cashier and you get some 1x$10, 2x$20, 1x$50 dollar chips (i.e. zPIV). This means that you no longer own that particular 100 dollar bill you exchanged and instead have “proof” that you still own $100. Now when you need 50 dollars of it back as fiat (PIV), you give your chips (zPIV) back to the cashier and the cashier delivers a brand new uncirculated 50 dollar bill to a recipient of your choosing.

zPIV Minting & Spending Process

In this example, Kirby wants to send PIV to Heidi using the Zerocoin protocol to anonymize the transaction.


PIVX - HOW ZEROCOIN PROTOCOL WORKS
@mcl4m, @fuzzbawls, @presstab, @rhubarbarian, @s3v3nh4cks, @spock
September 19, 2017
Kirby
Zerocoin Protocol
Heidi
Want to send 999 untraceable PIV to Heidi, and currently have 0 zPIV
Request to mint 999 zPIV
See PIV balance decrease by 999, and zPIV balance increase by 999
Spend 999 zPIV on Heidi
See zPIV balance decrease by 999
Convert 999 PIV to 999 zPIV
Denominations minted:
1x 500 zPIV
4x 100 zPIV
1x 50 zPIV
4x 10 zPIV
1x 5 zPIV
4x 1 zPIV
Receive and verify secret knowledge (zPIV) that proves ownership of PIV
Create 999 PIV at Heidi's address
See PIV balance increase by 999
Received 999 untraceable PIV from Kirby

Step by step Minting Process

1. Kirby initiates a request to mint 960 zPIV.
2. Zerocoin Protocol converts Kirby’s 960 PIV to the equivalent amount of zPIV, using the largest available zPIV denominations.
    1. Behind the scenes, Kirby has been given secret knowledge proving ownership of this mint (a unique serial number that is used by Zerocoin Protocol to track ownership of specific zPIV denomination amounts).
3. Kirby’s balance is updated accordingly
    1. With a 960 decrease in PIV, and a 960 increase in zPIV.

    2. Kirby also sees that the 960 zPIV is comprised of the following denominations that have been added: 1x 500 zPIV, 4x 100 zPIV, 1x 50 zPIV, 1x 10 zPIV.

Step by step Spending Process

1. Kirby initiates a send of the 960 zPIV to Heidi's PIVX address.
2. Zerocoin Protocol receives and validates Kirby's secret knowledge that proves ownership. Once used, the original minted balance cannot be re-spent.
3. Zerocoin Protocol creates 960 PIV at Heidi's PIVX address.
    1. Heidi receives 960 PIV from an anonymous sender.
    2. Kirby's balance is updated accordingly — with a 960 decrease in zPIV.

Denominations Explanation

To improve its transaction efficiency while retaining a high level of complexity, PIVX has implemented a set of integer based common denominators for the coin (PIV) amounts that gets converted into a pool of coins as zPIV. (much like the casino chips example above)

The denominations used by zPIV are: 1, 5, 10, 50, 100, 500, 1000, and 5000. Using this set of denominations provides a good balance of simplicity, usability, and security. The ultimate way to reduce traceability would only use 1 denomination (i.e 1 zPIV), however, it is not very practical to do that, as large transactions would require a huge amount of coins.

Using a very large set could potentially increase traceability to an insecure level, thus it was settled on a set of 8 possible coin denominations. This set is seen as a 'sweet' spot since it neither includes coins that are considered as too low or too high in a denomination. As the value of PIV changes, it's conceivable that we will extend or change this set to meet users needs.

When you spend your zPIV, you will simply have a proof that you have a coin of that denomination which includes other zPIV mints of that denomination.

This means that all zPIV redemption will be made in whole numbers (with change being issued for decimal amounts) thus making it near impossible to match before zPIV and after zPIV amount from 2 different addresses while there are many other identical zPIV to PIV transaction amounts being made.

Denomination Logic

When minting (converting) or spending (sending) zPIV, each algorithm will automatically determine the denominations used.

When spending (sending) zPIV to a PIVX address, following algorithm will automatically determine the denominations used from the user's

1). If you have the exact amount then start with largest possible denomination and go down until you reach the total

2) Otherwise : Minimize Spends (a) find the next denomination higher than the spend amount (if possible) and use that if available, (b) if not available start with the larger denominations and go down until you reach an amount just over what is needed
3) Or: Minimize Change. If not exact, try to find the amount above what is needed that minimizes how many coins you receive in change

Auto Minting

The privacy of zPIV becomes more effective when there are more of each denomination minted from many different sources. So to ensure its effectiveness, PIVX wallet has a feature to auto mint (convert) a configurable amount of PIV from the wallet's balance into zPIV without the need to manually convert.

Automint starts when the wallet/daemon is started, the wallet is unlocked (either fully or staking only) and the blockchain is synced. This means that if your wallet is encrypted and locked, the auto-mint feature will not engage. When the wallet is unlocked, it will still not touch any UTXO that are locked such as those that are used as collateral for masternodes.

– default percentage: 10%. Can be changed via GUI or via command-line option `-zeromintpercentage=<n>` or pivx.conf `zeromintpercentage=<n>`must not be less than 10%.

– default state: Activated. Can be deactivated (e.g. for exchanges) via command-line option `-enablezeromint=0` or pivx.conf `enablezeromint=0`

User can now configure a preferred denomination for Automint via UI, command-line option `-preferredDenom=<n>` or pivx.conf `preferredDenom=<n>` <n> is either one of the available denominations `1/5/10/50/100/500/1000/5000` or `0` (means no preference at all and let Automint do whatever it wants).

If there are not enough coins available for the preferred denomination Automint waits until there are enough coins available.

With each incoming new block, it does:

1. Check how much mintable coins are available.
    1. This excludes immature coins and locked coins (e.g. from masternodes)
2. Check how much Zerocoin/zPIV is available
3. Check if the percentage is below the target percentage

If the percentage is below the target percentage, it does:

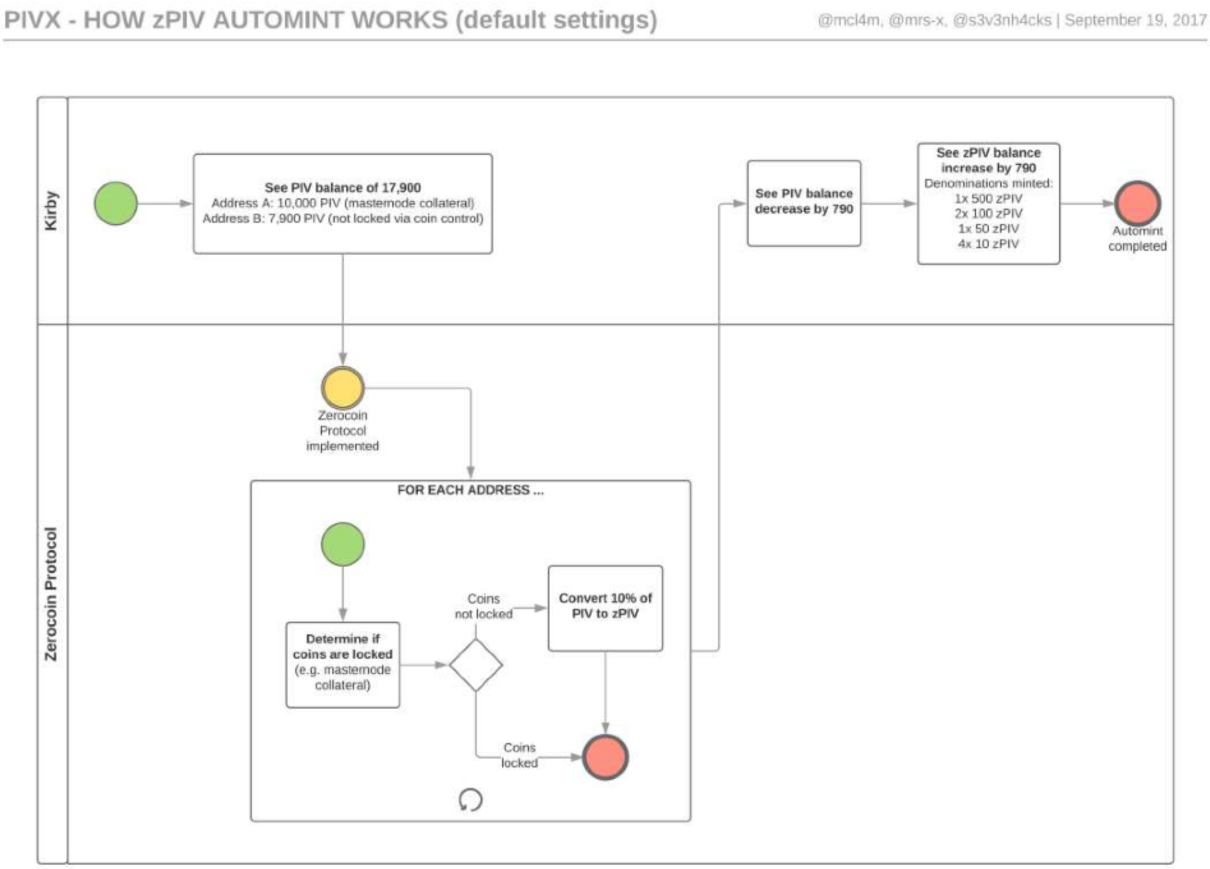
1. Calculate how many PIV needs to be converted to zPIV, e.g. 2015
2. Use the next smaller denomination (here 1000 PIV) and mints 1000 zPIV
3. Rinse and repeat until enough zPIV are minted.

In my example above the first incoming block would trigger minting 1000 zPIV, the next one again 1000 zPIV, the third one 10 zPIV and the fourth one 5 zPIV (assuming that no new incoming PIV change the base amount of available PIV).

The reason to use the next smaller denomination, and to only use one denomination per block is performance, exact denominations do not need to be broken down into exact denominations obviously, and one single mint can be done in a reasonable time. Exception: if a large amount of PIV needs to be minted, we use NOT our biggest denomination of 5000 PIV but 6666 PIV to have a more even distributions of available denominations (6666 = 5000 + 1000 + 500 + 100 + 50 + 10 + 5 + 1, which are our 8 available denominations).

zPIV Automint Process

(based on default settings)


PIVX - HOW zPIV AUTOMINT WORKS (default settings)
@mcl4m, @mrs-x, @s3v3nh4cks | September 19, 2017
Kirby
See PIV balance of 17,900
Address A: 10,000 PIV (masternode collateral)
Address B: 7,900 PIV (not locked via coin control)
See PIV balance decrease by 790
See zPIV balance increase by 790
Denominations minted:
1x 500 zPIV
2x 100 zPIV
1x 50 zPIV
4x 10 zPIV
Automint completed
Zerocoin Protocol
Zerocoin Protocol implemented
FOR EACH ADDRESS ...
Determine if coins are locked (e.g. masternode collateral)
Coins not locked
Convert 10% of PIV to zPIV
Coins locked

1. Kirby, prior to the launch of Zerocoin Protocol, has a balance of 17,900 PIV. He owns a masternode, so 10,000 PIV of his balance is held at the masternode's dedicated address and locked as collateral. Kirby has not used Coin Control to lock the remaining 7,900 PIV.
2. Zerocoin Protocol is implemented..
3. Zerocoin Protocol processes each and every address individually as follows:
    1. Determine if the coins are locked.

    2. If the coins are not locked, convert 10% of PIV to zPIV.
    3. If the coins are locked, do nothing.

4. Kirby sees that his balance has decreased by 790 PIV, which equates to 10% of his coins that are not locked.
5. Kirby also sees that his balance has increased by 790 zPIV. Since he has not specified any zPIV denomination preferences, he now has the following denominations available to spend:

- 1x 500 zPIV
- 2x 100 zPIV
- 1x 50 zPIV
- 4x 10 zPIV

Spend Security Level

When spending zPIV denominations, a user is prompted to enter a *Security Level* choosing from 1-100. In an indirect way, the Security Level parameter allows the user to choose how many coins to obfuscate their transaction with.

A Security Level of 1, for example, would take all of the minted coins in the blockchain before your mint was added to the blockchain, and would then add any coins that were minted within the next 10 blocks as well. A Security Level of 2 would do the same thing, except add the next 20 blocks worth of mints. A Security Level of 100 will add the maximum amount of mints up to the current end of the blockchain.

The higher the Security Level, the more computation and time it will take to spend. Although it takes longer, a level of 100 is recommended for transactions that need maximum anonymity.

Handling of Change

As zPIV is made up of fixed denominations, there will be times when the amount needed to be spent cannot be made up by existing denominations. For example, if you have a single 1000 zPIV denomination but you want to send 985 PIV to an address, there will be a difference of 15 PIV that will be received back as change. This change can compromise the privacy of the transaction as it can lead back to your existing address if you mistakenly mix your change back in with your other PIVX addresses.

In order to prevent this, there are 2 methods that can be used. First option is the use of the built-in feature that automatically converts the change back into zPIV. This will spend the zPIV into the required amount of PIV to the target address, then mint the remaining change of PIV back into zPIV. This is the most convenient method. However, the amount of change that is not convertible to a denomination (the lowest denomination available is 1) will be converted to a fee.

The second option is to issue change to a standard PIVX address, which leaves you up to handling the segregation of that Piv from your day-to-day Piv balance. This option can lead to mistakes and is not recommended if anonymity is important for the transaction.

zPIV Data Integrity

Every minted zPIV denomination is associated with a unique serial number that is stored in the local wallet.dat and not on the blockchain. This means that when a new zPIV denomination is minted, the wallet.dat should be backed up as the previous backup will not have the serial numbers for the newly minted zPIV denominations.

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.

Due to its local database design, it is imperative that your wallet is backed up after every new zPIV mint to ensure that your denomination serial numbers are up to date.

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.

Authors

Written by: jakiman, mcl4m
Technical input by: spock, presstab, fuzzbawls, mrs-x

REFERENCES

[1] https://en.wikipedia.org/wiki/RSA-2048