VSYNC

THE NEXT GENERATION OF MONEY

COMMUNITY DRIVEN CRYPTOCURRENCY

WHITE PAPER
2018

CONTENTS

INTRODUCTION

VSYNC is a cutting edge, decentralized cryptocurrency unlike any other in the market. Our currency offers complete privacy, security, reliability and faster transactions to revolutionize the way monetary values are exchanged.

Most importantly to our success, VSYNC is community-driven. Our mission is to bring the powerful capabilities and endless possibilities of cryptocurrency to the masses. A paradigm shift is occurring and the technologies we describe here will be the driving force behind it. We believe in fair distribution, total transparency, and complete decentralization. That's why we created an open source, privacy-focused cryptocurrency that offers anonymized transactions.

This white paper outlines the technical aspects of VSYNC, the numerous benefits it provides, and how it solves the current issues with major cryptocurrencies like Bitcoin. Finally, it highlights the VSYNC development roadmap through 2019 to give you an idea of what's in store for this exciting new cryptocurrency.

VSYNC is a currency for everyone. We invite you to become part of our friendly, enthusiastic, and open community.

WELCOME TO THE NEXT GENERATION OF MONEY.

ABOUT VSYNC

VSYNC is a decentralized cryptocurrency that utilizes the latest and most advanced technology in blockchain, to ensure a highly reliable and secure network.

Inspired by projects like Bitcoin, the VSYNC currency (VSX) connects a variety of smart features together to provide a cutting-edge cryptocurrency with capabilities and benefits not yet seen in the vast majority of other cryptocurrencies. VSYNC is an open source, completely private PoS cryptocurrency based on Bitcoin Core 0.15.x and DASH.

VSX offers anonymized transactions utilizing the ZeroCoin protocol. It also allows for instant transactions featuring guaranteed zero confirmation transactions using SwiftTX.

- **Transactions are completely anonymous**
- **Coin balance is hidden and can't be linked to any particular address**
- **Transaction history is hidden**
- **Source & target address are not visible**

- **Super fast transactions: it takes as little as 0.5 seconds to mint and 2.5 seconds to spend**

- **Ability to send a fully transparent transaction 24/7**

VSX also features decentralized blockchain voting, providing for consensus-based development of the current Masternode technology. Enabling us to secure the network and provide the above features. Each of these Masternodes is secured with 100 000 VSX in collateral.

The VSYNC platform aims to continuously innovate and expand to offer a wide variety of features and functionalities. We are dedicated to remaining actively engaged within the VSYNC community, in order to maintain a high level of transparency and build a solid trust network with our investors and supporters. VSYNC has a fair distribution and will continue to develop realistic and progressive goals for our platform.

We have a phenomenally active and dedicated development team to keep our code well-maintained. Our team is passionate about delivering the best possible cryptocurrency platform and bringing this technology to consumers around the world.

PRIVATE.

SECURE.

DECENTRALIZED.

ANONYMOUS.

INSTANT.

THE DRAWBACKS OF BITCOIN

Bitcoin is the pioneer cryptocurrency, it does have a few significant flaws. Here, we identify some of the deficiencies of Bitcoin and explain how VSYNC solves these issues.

LACK OF PRIVACY & ANONYMITY

All Bitcoin transactions are completely visible on the blockchain; anyone can see the addresses involved in a transaction and the exact nature of the transaction (e.g. which address sent funds, which address received funds). This means that Bitcoin transactions are traceable, it compromises privacy if a certain address becomes linked to a user's identity.

CENTRALIZED

Bitcoin uses the Proof of Work (PoW) system rather than the PoS system. As previously mentioned, PoW systems are also more difficult to participate in, as miners are required to perform more difficult work, with higher hardware and electricity costs. This means that because there are greater obstacles to ownership in the PoW system, Bitcoin is much more centralized – the majority of Bitcoin is owned by only a few members (Saberhagen, 2013).

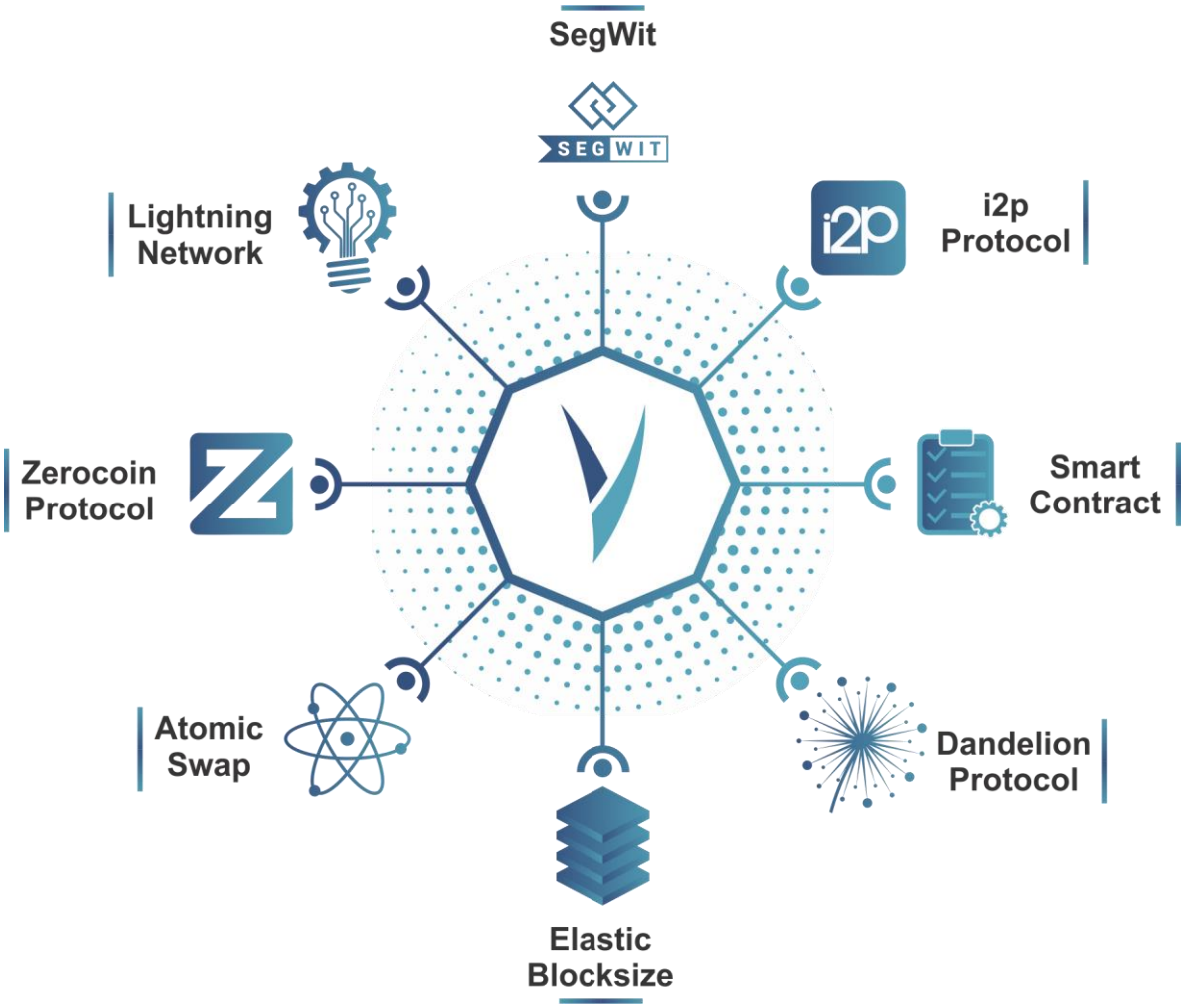
SLOW TRANSACTIONS & HIGH TRANSACTION FEES

The PoW system used by Bitcoin is also far less efficient than the PoS system. PoW systems are also more difficult to participate in, as miners are required to perform more difficult work, with increasingly exorbitant hardware and electricity costs. This results in slower transactions and higher transaction fees for users.

WHY VSYNC IS DIFFERENT

VSYNC (VSX) is a currency for everyone. It is instant, decentralized, and anonymous, with virtually zero fees. That means that anyone and everyone can use VSYNC, creating an open, inclusive global currency system.

VSYNC differs from other major cryptocurrencies in four main areas: privacy, security, decentralization, and speed. These four traits are enabled through VSYNC's unique, innovative implementation of the following protocols.



1 ZEROCOIN & I2P

VSYNC allows full anonymity, and thus full privacy for its users. With the ZeroCoin Protocol and implementation of networks like the I2P Network, all VSX transactions are untraceable and can never be linked to a particular user or tracked by a third party. This adds an extra layer of security, as it makes attacks difficult to mount.

2 THE DANDELION PROTOCOL

With the Dandelion Protocol, VSYNC provides total security. While many of VSYNC's components provide security, including ZeroCoin, I2P, smart contracts, and the Lightning Network, the Dandelion Protocol offers an alternative layer of protection for users' privacy, making senders' IP (Internet Protocol) addresses virtually untraceable.

3 SMART CONTRACTS & ATOMIC SWAP

VSYNC believes that the world of money should be decentralized. Rather than having all the power hoarded by a few individuals or groups, a decentralized currency puts the power in the hands of the masses. This allows protection from factors like corporate or government corruption as well as inefficiency. By eliminating the need for a central authority and thus a single point of failure, reliability and security is increased. Enabling decentralized transactions through smart contracts and atomic swap allows VSYNC to remain free and open to everyone.

4 SEGWIT, LIGHTNING & ELASTIC BLOCKSIZE

The traditional payment system which requires a third party to complete any transaction results in a great deal of inefficiency, delays and errors.

Decentralized currency erases those problems, allowing for more streamlined, faster transactions. SegWit and elastic block sizes allow higher capacity, meaning more transactions can be processed per second, and underlying data structures result in better confirmation times. Furthermore, VSYNC will enhance its transaction capacity by implementing the lighting network, a second layer protocol that enables scalable, instant transactions on the blockchain powered by smart contracts.

Detailed explanations of the function and features of each of these protocols are featured in the following sections.

Here's how VSYNC compares to other leading cryptocurrencies in the market, feature by feature:

SPECIFICATIONS

Algo: Xevan

Code Base: POS 3.0, Bitcoin Core 0.15.x

Masternodes: 100 000 Collateral

Difficulty Adjustment: Each Block Dark Gravity Wave v3

POW: Ends on block 259 200 / 180 days

POS: Starting from block 259 201

InstantTX: SwiftTX

Privacy Technology: ZeroCoin Protocol (zVSX)

RPC Port: 65 015

P2P Port: 65 010

PROOF OF STAKE

VSYNC is a Proof of Stake (PoS) cryptocurrency. PoS allows users to mine or validate block transactions according to the amount of coins that user holds. So, the more coins owned by a miner, the more mining power he or she has.

The main driving force behind the invention of PoS was to eliminate the major drawbacks of the PoW (Proof of Work) consensus mechanism. The PoS mechanism, which was originally invented by Sunny King and implemented in PeerCoin, essentially lets participants create and mine new blocks and receive a block reward by allowing their wallets to do automatic coin staking.

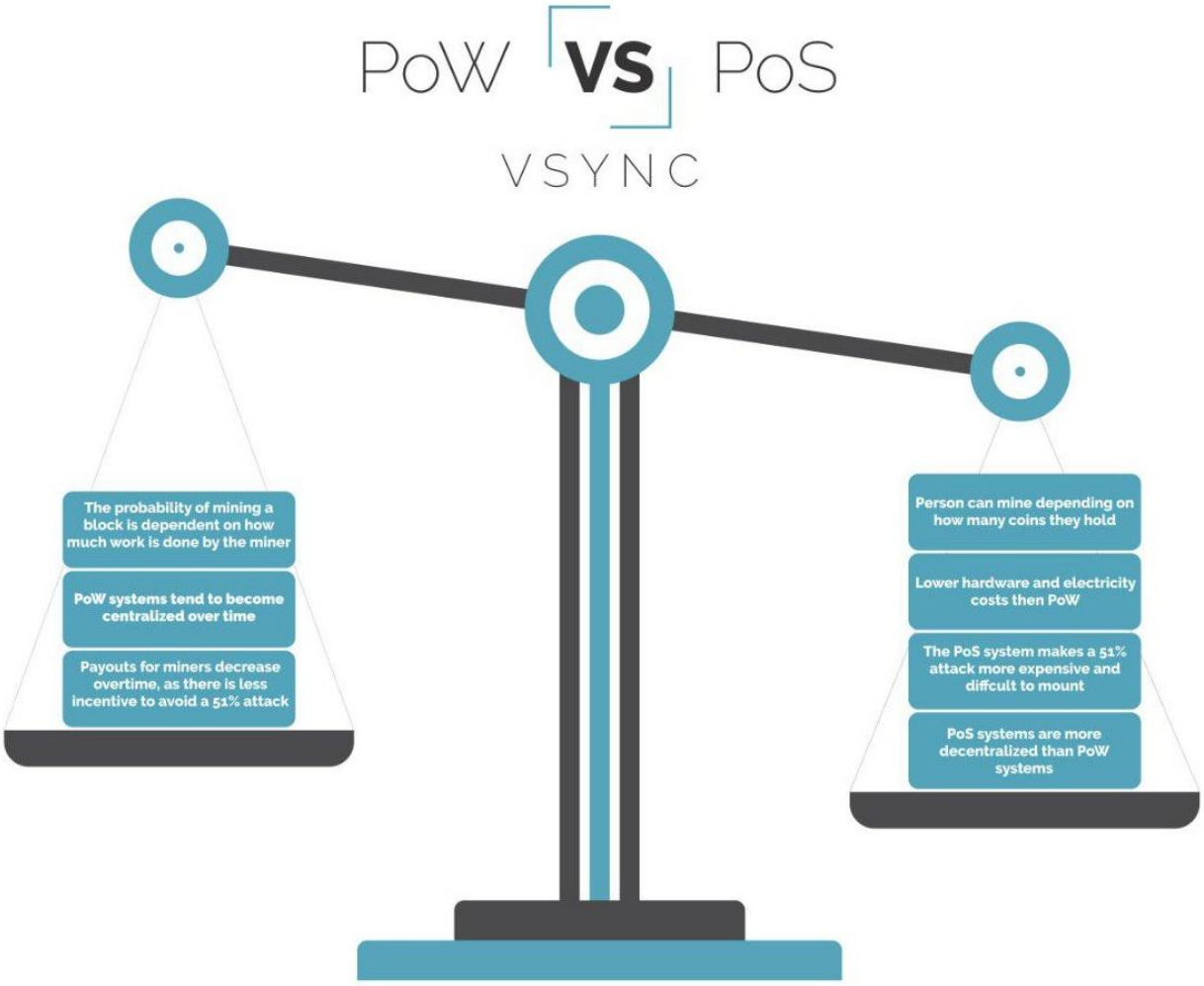
The ultimate objective of PoS is to make it impossible to counterfeit a block. Furthermore, bigger players should not get disproportionally bigger rewards while no member of the network has the ability to control the entire network.

Similar, to PoW, PoS has the notion of being a" lottery". The key difference between a lottery and PoS is that it is impossible to own more lottery tickets simply by changing some data in the block. Considering the block hash as the lottery ticket, PoS has the" kernel hash" concept, which is composed of many pieces of data which are not readily modifiable in the current block. Thus, miners do not have an easy way to modify the kernel hash, such as by simply iterating through a large amount of hashes.

As a distinction from PoW, the coin base transaction – which is the first transaction in the block – is empty and rewards no tokens. The stake transaction is the 2nd transaction in the block and rewards the stakers. Staking transaction rules make it easy to identify a stake transaction, giving the blockchain enough information to validate the block. It is important to note that most of the rules of PoW also apply for PoS blocks, including valid Merkle hash, valid transactions and timestamp within time drift allowance.

PoS has several advantages over Proof of Work (PoW). Firstly, it is more efficient. The electricity and hardware costs of PoS systems are considerably lower than that of a PoW system, which means that the system is not only more cost-effective, but more environmentally friendly.

Furthermore, as it is easier and less expensive to participate in a PoS system, more people are encouraged to become involved and run nodes. Thus, the system becomes more decentralized, as ownership of the network is split amongst a greater number of users, rather than a small few (Ray, 2017).

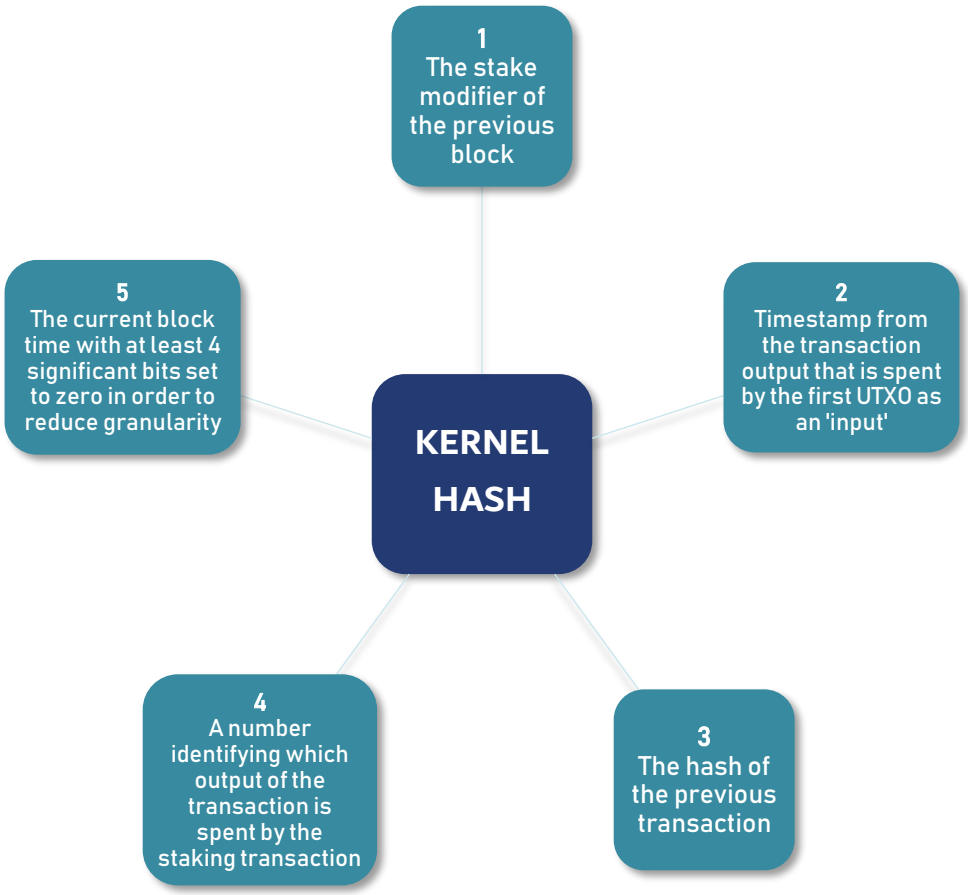


PROOF OF STAKE IN VSX

Since its introduction, PoS mechanisms have been improved and adapted accordingly (e.g., PoSv2 by Pavel Vasin PoS Velocity by Larry Ren, and CASPER by Vlad Zamfir). VSX is built upon Proof of Stake Version 3 (PoSv3) with considerable improvement over Version 2 by Pavel Vasin. Although there are some minor details that have been modified, the core consensus model is identical. The following subsections will detail the advantages of PoSv3 with respect to previous versions of PoS, along with the evolution history of PoS and a brief overview of the protocol structure and rules.

KERNEL HASH

The main data structure of kernel hash consists of:



The following pseudo code briefly explains the mining process of PoW:

```
while (blockhash > difficulty) {
        block. nonce = block. nonce + 1
        blockhash = sha256(sha256(block))
}
```

Whereas the pseudocode for finding a valid kernel hash is follows:

```
while (true){
        foreach (utxo in wallet) {
                blockTime = currentTime – currentTime % 16
                posDifficulty = difficulty ∗ utxo . value
                hash = hash (previousStakeModifier << utxo. time <<
                utxo. hash << utxo. n << blockTime)
                if (hash < posDifficulty) {
                        done
                }
        }
        wait 16s –– wait 16 seconds, until the block time can be changed
}
```

Multiple UTXOs are typically contained in a single wallet, the total amount of which is the balance. The number of coins in the staking transaction determines the difficulty level. This level is inversely proportional to the amount of coins subject to staking, discouraging users to create many tiny UTXOs for staking which would have a fatal effect on blockchain resource maintenance, as well as compromise overall security.

Once a valid kernel hash is found with one of the UTXOs which can be spent, a staking transaction can be created. This overall mechanism is briefly shown in the pseudo-code above.

The staking transaction will have at least two newly-created UTXOs as an output, in addition to the UTXO that is being spent as an" input". One of these output UTXOs (vout) is empty and identifies to the blockchain that there is a staking transaction, whereas the second one contains either an OP RETURN data transaction with a single public key or a pay-topubkey script.

After transactions are added to the block from mempool, a signature is created in order to prove that a valid PoS block has been approved. The public key that is encoded in the second vout of the staking transaction is used as the signature. After the signature is applied, the block can be broadcast to the network. Being validated by the nodes in the network, it is broadcasted to all other nodes to which it has a connection.

PoSv1

PoSv1, which was first employed by PeerCoin, is mainly based on the notion of" coin age". Coin age refers to how long a UTXO has not been spent on the blockchain. Coin age is used as a factor to increase the weight of unspent coins over time and reduce the difficulty level.

The implementation of PoSv1 results in the decrease of difficulty if the coin age is higher. The primary negative side effect of this approach is that it encourages users to open their wallets at longer intervals, which essentially makes it easier to execute double-spending attacks. PeerCoin, the first coin which made use of PoS, eliminated this side effect by becoming a hybrid blockchain of PoW and PoS.

PoSv2

Although PoSv2 introduced numerous changes to PoSv1, the most important change is that coin age has been removed from consensus, with a different stake modifier mechanism employed. PoSv2 implementation encourages nodes to be online longer in order to get their stake rewards. This ultimately provides a safe consensus mechanism that mitigates various attacks without a requirement for a PoS/PoW hybrid blockchain.

PoSv3

It is inaccurate to consider PoSv3 as new version of PoSv2 with only incremental improvements. While previous block time was included in the stake modifier for PoSv2, it was removed to prevent" short-range" attacks. In short-range attacks, an alternative blockchain is mined by iterating through previous block times. In PoSv2, instead of coin age, block and transaction times are used to determine the age of UTXO. Unlike coin age, there are minimum confirmations required before UTXO can be used for staking.

However, in PosV3, the age of UTXO is determined by its depth in the blockchain as a simplified mechanism. This mechanism prevents the use of incorrect timestamps on the blockchain, making the system more immune to time warp attacks. With PoSv3, support for OP RETURN coin stake transactions was added, allowing a new UTXO to be created as an output. This new UTXO contains the public key to sign the block without the need for a full pay-to-pubkey script.

PoW REWARDS

BLOCK	REWARD	MINER	MN	BUDGET
2-43200	**225** VSX	**180** VSX	**45** VSX	N/A
43201-151200	**255** VSX	**157.5** VSX	**45** VSX	**22.5** VSX
151201-259200	**80** VSX	**36** VSX	**36** VSX	**8** VSX

PoS REWARDS

	BLOCK	REWARD	MN	POS	BUDGET
PHASE 1	**259201-302399**	**75** VSX	**52.5** VSX	**22.5** VSX	N/A
PHASE 2	**302400-345599**	**67** VSX	**46.9** VSX	**20.1** VSX	N/A
PHASE 3	**345600-388799**	**59** VSX	**41.3** VSX	**17.7** VSX	N/A
PHASE 4	**388800-431999**	**51** VSX	**35.7** VSX	**15.3** VSX	N/A
PHASE 5	**432000-475199**	**43** VSX	**30.1** VSX	**12.9** VSX	N/A
PHASE 6	**475200-518399**	**35** VSX	**24.5** VSX	**10.5** VSX	N/A
PHASE 7	**518400-561599**	**27** VSX	**18.9** VSX	**8.1** VSX	N/A
PHASE 8	**561600-604799**	**19** VSX	**13.3** VSX	**5.7** VSX	N/A
PHASE 9	**604800-647999**	**11** VSX	**7.7** VSX	**3.3** VSX	N/A
PHASE X	**648000-Infinite**	**3** VSX	**2.1** VSX	**0.9** VSX	N/A

SWIFTTX

Another feature of VSYNC is SwiftTX. SwiftTX is used in order to provide fast transactions featuring guaranteed zero confirmation transactions.

SwiftTX ensures transaction confirmation in seconds. This means that the transacted funds will be available instantly, so you'll be able to spend your money right away without having to wait for multiple confirmations to ensure that the transaction was valid.

SwiftTX transactions are guaranteed by the network of masternodes, which will be discussed below.

MASTERNODES

The VSYNC platform has decentralized blockchain voting providing for consensus-based advancement of current Masternode technology. This is used to secure the network and provide the features described in the About VSYNC section.

A masternode is a cryptocurrency node or wallet that keeps a full, real-time copy of the blockchain at all times and performs special functions that regular nodes do not (Khatwani, 2018). For instance, in addition to keeping the blockchain and relaying blocks and transactions, masternodes participate in the governance of the blockchain network through a voting system. They also increase privacy of transactions and allow instant transactions.

With 100 000 VSX, you can create your own masternode, increase the network health and support our transactions. The 100 000 VSX is used as collateral to secure the Masternode, so that the owner and the operator are discouraged from compromising or corrupting the system.

We believe that every member of our community should have a voice. Therefore, VSYNC improves upon the existing masternode voting system found in other cryptocurrencies by allowing the network to be governed by the entire community, creating a decentralized democratic system (Merkle, 2017). In typical blockchain systems, only masternode owners are given the ability to vote and make decisions for the community. With VSYNC, voting power is decentralized, so every single VSX holder has the power to vote, regardless of whether they own a masternode.

SMART CONTRACTS

Smart contracts are the core of the decentralized blockchain network. They enable private and secure transactions to occur on the blockchain without the need for a third party or central authority; these contracts are self-executing according to the terms of agreement between the buyer and seller, which have been written directly into lines of code on the blockchain.

Smart contracts allow each party to remain anonymous as well as ensure that the agreement between two parties will be honoured, so both the buyer and seller is protected. Once the contract has been signed, the transaction is irreversible. The smart contract not only defines the rules of an agreement and its penalties, but automatically enforces them (Rosic, 2017). Transactions are also traceable, as they will be visible on the public ledger (with the individual parties remaining anonymous). Thus, smart contracts are safe, reliable, conflict-free and completely private.

We will use smart contracts on our network to enhance the process of buying and selling and allow for true integration into mainstream commerce.

ZEROCOIN PROTOCOL

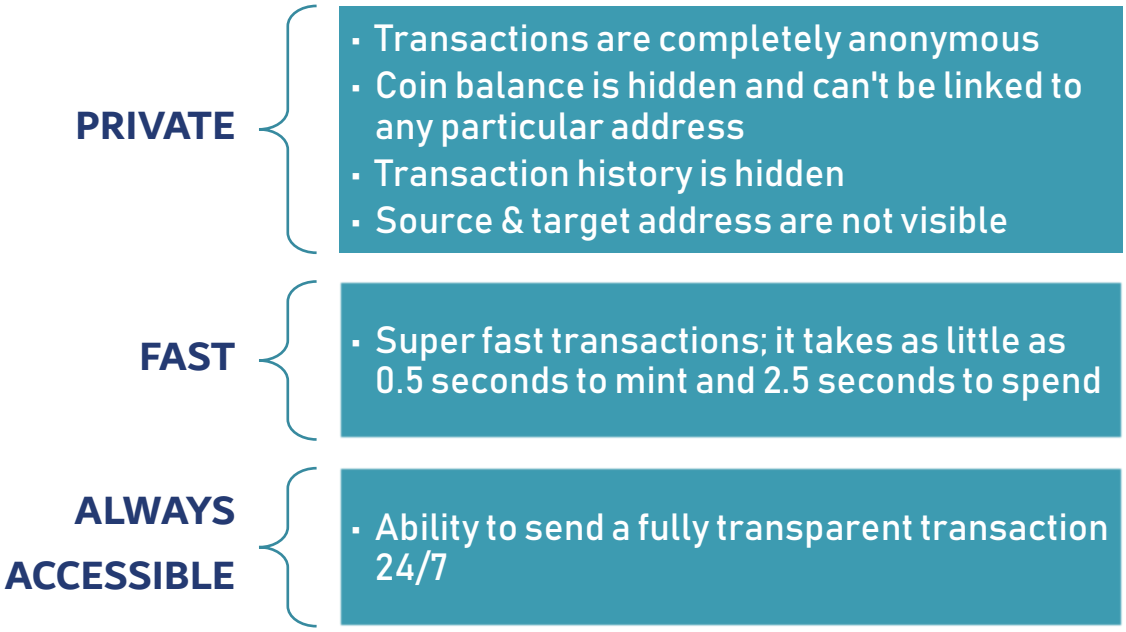
VSYNC will be implementing the ZeroCoin Protocol to enable direct, anonymous payments between parties. The ZeroCoin Protocol is a bitcoin extension that functions similarly to a coin mixer, provisionally pooling coins together in exchange for a temporary currency called zerocoins (Miers, Garman, Green, & Rubin, 2013). This protocol anonymizes exchanges to and from the laundering pool with the use of cryptography and records the transactions within the blockchain, making it private and safe, as well as eliminating any reliance on third parties (PIVX, 2017).

The cryptographic principles used in ZeroCoin in order to allow full anonymity involve separate zerocoin mint and spend transactions. This works in the following way (Miers, Garman, Green, & Rubin, 2013):

1. A person generates a random serial number S.
2. This number is encrypted (or committed) into a coin C by use of a second random number r.
3. The coin C is added to a cryptographic accumulator by miners; at the same time, an amount of bitcoin equal in value to the denomination of the zerocoin is added to a zerocoin escrow pool.
4. The owner of the coin needs to prove two things by way of a zero-knowledge proof in order to redeem the zerocoin into bitcoin. (Zero-knowledge proof: a method by which one party can prove to another that a given statement is true, without conveying any additional information.)
    a. The first thing the coin owner must prove is that they know a coin C that belongs to the set of all other minted zerocoins (C1, C2… Cn), without revealing which coin it is. This can be done quickly by using a one-way accumulator that does not reveal the members of the set.
    b. The second thing that must be proven is that the person knows a number r, that along with the serial number S, corresponds to a zerocoin.
5. The proof and serial number S are then posted as a zerocoin spend transaction.
6. Miners verify the proof and that the serial number S has not been spent previously.
7. The transaction is posted to the blockchain upon verification.
8. The amount of bitcoin equal to the zerocoin denomination is transferred from the zerocoin escrow pool.

Note: Zerocoin transactions ensure anonymity because the minted coin C is not linked to the serial number S used to redeem the coin.

THE BENEFITS OF ZEROCOIN



I2P NETWORK

VSYNC will utilize the I2P Network (Invisible Internet Project), which uses a fully peer to peer decentralized model offering VSYNC users full privacy protection as they communicate over the Internet.

I2P is an anonymous overlay network that allows for peer to peer communication completely free from censorship. It was designed to protect communication from dragnet surveillance and monitoring by third parties, in order to make attacks more and more difficult to mount (The Invisible Internet Project). The I2P Network is more robust, more secure and much faster than other anonymous communication software models such as Tor. It is also free and open source.

The network – enabled by the I2P router – encrypts users' traffic with end-to-end encryption and sends it through a volunteer-run network of approximately 55,000 computers (called "I2P nodes") distributed globally. This ensures fully anonymous connections. Furthermore, the connections are practically untraceable by third parties, as there is such a large volume of paths that the traffic can transit. As the I2P network grows in size, the anonymity it offers will become even stronger.

DANDELION PROTOCOL

The Dandelion Protocol offers an alternative layer of protection for users' privacy, making senders' IP (Internet Protocol) addresses virtually untraceable. This protocol, designed by the Zcash advisor and developer Andrew Miller and a team of researchers from the University of Illinois, prevents blockchain analysis from linking IP addresses to wallet addresses.

The Dandelion Protocol is a brand-new method of broadcasting transactions aimed at prohibiting anyone from being able to locate IP addresses. It was developed as a "privacy-enhancing modification to Bitcoin's transaction propagation mechanism" (Redman, 2017). Transactions implemented with the Dandelion Protocol are relayed to nodes, which then bounce between several more locations – referred to as "hops" – before a symmetric broadcast is sent to other nodes, who are unable to identify the original IP source (Butinx, 2017).

Dandelion works in the following two phases, as detailed in the Github proposal (Redman, 2017):

1. The first phase is the "stem" phase. During the stem phase, each node relays the transaction to a single peer, which then follows a random number of hops along the stem.
2. This is followed by the "fluff" phase, which behaves identically to flooding/diffusion. Even if an attacker is able to find the location of the fluff phase, it would be extremely difficult to identify the source of the stem.

Dandelion provides additional privacy and security to the VSYNC community by obscuring the original source IP of each transaction to further protect users from attacks.

SEGWIT

VSYNC will be implementing SegWit (short for Segregated Witness) to our network in order to make VSYNC a scalable payment system that accommodates a high volume of users and transactions. SegWit is a protocol upgrade that allows the number of transactions per block on VSYNC's network to be increased by changing the way that data is stored. It was first activated on litecoin in May of 2017, then later on bitcoin in August 2017.

SegWit was created as a solution to bitcoin's scaling issue – in the main protocol for bitcoin, the maximum block size is 1MB, restricting the number of transactions that bitcoin can process to about 7 per second (Acheson, 2018). This provided a significant obstacle to the potential growth of bitcoin.

The SegWit protocol upgrade enables a greater number of transactions to be completed per second, in addition to solving transactions malleability. Transaction malleability allowed anyone to modify the transaction id and its subsequent hash by changing small details. This prevented the development of more complex features like smart contracts and second-layer protocols.

SegWit provides a solution to the issue of transaction malleability by removing the signature information and storing it in another location outside of the base transaction block. Therefore, if signatures and scripts are modified, it does not affect the transaction ID. It also means that transactions weigh significantly less without signature information, so more are able to fit into a block, which enables a greater number of transactions to be processed on a smaller block size.

ELASTIC BLOCK SIZE

While SegWit does not increase the block size limit – it only increases the number of transactions that can be processed within a 1MB block – VSYNC will implement the elastic block size mechanism to further increase VSYNC's scalability and usability.

Elastic block size is a block size mechanism that allows blocks to expand on their own to incorporate variations in sizes. The size of blocks in the VSX network will automatically adjust on demand to assure the best possible user experience, as well as ensure that VSX will be able to scale on mass consumer adoption.

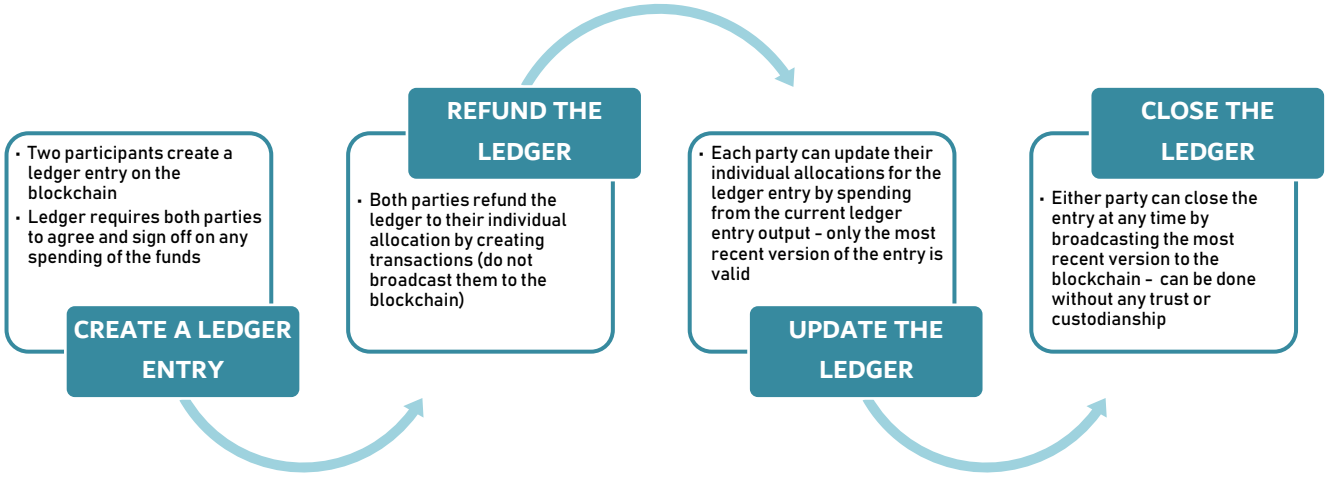
LIGHTNING NETWORK

VSYNC will further boost its transaction capacity by implementing the lighting network, a second layer protocol that enables scalable, instant transactions on the blockchain powered by smart contracts (Lightning Network). Lightning is a decentralized network, allowing instant payments across a network of participants using smart contract functionality.

The lightning network utilizes the blockchain's underlying technology, with real blockchain transactions and native smart-contract scripting language, in order to create a secure network of users who are able to complete high-speed, high-volume transactions.

LIGHTNING NETWORK

BIDIRECTIONAL PAYMENT CHANNELS



Similarly, to network packets in Internet routing, paths are created across the network through these bidirectional ledger entries, with nodes along the path. These nodes are not trusted, as the payment is self-enforced and executes according to the script. This script enforces atomicity via decrementing time-locks (more on this below, in 'Atomic Swap.')

THE BENEFITS OF LIGHTING TRANSACTIONS

Instant. The lightning network enables high-speed payments without the wait for block confirmation, as security is enforced by smart contracts (on or off the blockchain). The speed of lightning transactions varies from milliseconds to seconds.

Cross-Chain. Atomic swaps can occur off-chain while maintaining heterogeneous blockchain consensus rules, making it possible to make transactions across blockchains without trust in third party custodians.

High Capacity. The lightning network is capable of supporting anywhere from millions to billions of transactions per second, with attaching payment per action/click now possible without custodians.

Low Cost. By transacting and settling off-blockchain, lightning transactions allow transactions to be made with exceptionally low fees, allowing for greater flexibility in making payments (for instance, micropayments).

ATOMIC SWAP

The implementation of Atomic Swap on VSYNC's network allows VSX and other currencies to be traded in a safe, trusted exchange between two parties. Atomic Swap eliminates the need for an Escrow or any third party centralized app, allowing safer, more secure and faster exchanges.

Atomic Swap is the exchange of one cryptocurrency to another cryptocurrency without the dependency on a third party (Madeira, 2018). In an atomic swap, two parties with two different types of currencies can trade directly with one another. For instance, someone who holds Litecoins but wants bitcoins can make a trade with an owner of bitcoins without the need to go through a third-party exchange.

HASH TIME-LOCKED CONTRACTS

To ensure that the transaction is safe – i.e. one party cannot accept the other party's coins and then fail to send their own coins – atomic swaps use hash time-locked contracts (HTLCs). HTLCs guarantee a completely trustless atomic swap by automatically enforcing the requirements of the trade (like smart contracts). HTLCS require the recipient to generate a cryptographic proof of payment prior to a certain deadline acknowledging that they have received the payment or risk losing the right to claim that payment (i.e. the funds will be sent back to the sender). So, to claim the funds sent by the other party, the recipient produces a number that only they know in order to generate the cryptographic hash. In order for the other party to then claim their funds, they must also provide the number that was used to generate this hash.

ROADMAP

The VSYNC team has developed a roadmap to guide the project's expansion. The roadmap is subject to changes. Here's what the next 2 years will look like for us:

2018

Q1

Logo Rebranding
Logo rebranding for VSYNC.

New wallet update
We are updating our GUI software and are updating a few files for future features.

New Website
New website with all our new information on VSYNC.

White Paper
Our new white paper will be published in a range of different languages.

Expanding Official Team
Official announcements of new employees to the VSYNC team. This will continue throughout 2018.

Q2

Ad. Campaign
We will be placing ads all over the Crypto space promoting VSYNC. This will continue throughout 2018.

Listing on Exchanges
We will be actively seeking new exchanges. This will continue throughout 2018.

Merchandise Acceptance
Online stores start accepting VSYNC for payment.

Official Subreddit
Getting our reddit community together making posts and sharing ideas.

Q3

Paper Wallet
Opening our paper wallet website, enabling you to lock your funds offline in a safe place.

Mobile Wallet
Mobile android wallet release, in order to monitor your funds on the go.

Community Forum Launch
Community forum where we can get together, chat, share ideas and more.

Q4

Wallet Design & Core Update 0.12.1
The VSYNC core development team will be continually maintaining and updating VSYNC's code to ensure we are in sync with Bitcoin functionality and features.

Masternode Sharing Service
Building a website to enable masternode sharing for the community.

ZeroCoin Protocol
ZeroCoin allows direct anonymous payments between parties.

Governance Voting
Allowing users to vote on team decisions and proposals.

2019

Q1

Masternode Auto Setup
Users will be able to easily setup a masternode from within the QT wallet user interface.

In Wallet Proposal Tab

Users will be able to easily perform governance functions from within the QT wallet user interface.

In Wallet Voting Tab

Users will be able to easily to vote for all VSX proposals from within the QT wallet user interface.

Q2

Elastic Blocksize

Block size will automatically adjust on demand to ensure the best user experience. VSX will be able to scale on mass consumer adoption.

I2P Network Integration

I2P network uses a fully peer to peer decentralized model. More robust, more secure and much faster than other models such as Tor.

Listing on decentralized exchanges

VSYNC will be working hard to have VSX listed on decentralized exchange. This will continue throughout 2019.

Q3

Dandelion Protocol

Alternative layer of protection for user's privacy making senders' IP addresses virtually untraceable. Prevents blockchain analysis from linking IP addresses to wallet addresses.

Segregated Witness (SegWit) Integration

We are adding SegWit to our network, which allows the numbers of transactions per block on VSYNC's network to be increased.

Continued Team Recruiting

We will continue to look for new members for our team. This will continue throughout 2019.

Q4

Lightning Network

Lightning is a decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants.

Atomic Swap

Implementation of Atomic Swap to VSYNC's network allowing VSYNC and other currencies to be traded in a safe, trust less exchange between two parties. Atomic swap eliminates the need of an escrow or any third party centralized app allowing safer, secure and faster exchange.

Smart Contract Implementation

We will start using smart contracts on our network, enhancing the process of buying and selling and allowing for true integration into mainstream commerce.

REFERENCES

(n.d.). Retrieved from The Invisible Internet Project: https://geti2p.net/en/

(2017). Retrieved from TokenPay.com.

Acheson, N. (2018, February 22). *What is SegWit?* Retrieved from Coindesk: https://www.coindesk.com/information/what-is-segwit/

Butinx, J. (2017, June 18). *What is the Dandelion Anonymization Proposal?* Retrieved from The Merkle: https://themerkle.com/what-is-the-dandelion-anonymization-proposal/

Khatwani, S. (2018, February 19). *What Is A Masternode And How Is It Useful For Cryptocoin Investors.* Retrieved from CoinSutra: https://coinsutra.com/masternodes/

Lightning Network. (n.d.). Retrieved from Lightning Network: https://lightning.network/

Madeira, A. (2018, February 28). *What Are Atomic Swaps?* Retrieved from CryptoCompare: https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/

Maxwell, G. (2013, August 22). *CoinJoin: Bitcoin privacy for the real world.* Retrieved from https://bitcointalk.org/index.php?topic=279249

Merkle, T. (2017, March 26). *PIVX Provides an Instant, Private and Community Designed Governance Alternative to Dash.* Retrieved from The Merkle: https://themerkle.com/pivx-provides-instant-private-alternative-to-dash/

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). *Zerocoin: Anonymous Distributed E-Cash from Bitcoin.* Retrieved from The Johns Hopkins University Department of Computer Science: http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

PIVX. (2017, October 16). *PIVX Zerocoin (zPIV) Technical Paper.* Retrieved from PIVX: https://pivx.org/zpiv/

Ray, S. (2017, October 6). *What is Proof of Stake?* Retrieved from Hacker Noon: https://hackernoon.com/what-is-proof-of-stake-8e0433018256

Redman, J. (2017, June 16). *New Dandelion Proposal Aims to Anonymize Bitcoin Transaction Broadcasts.* Retrieved from Bitcoin.com: https://news.bitcoin.com/dandelion-bitcoin-anonymize-transaction-broadcasts/

Rosic, A. (2017). *Smart Contracts: The Blockchain Technology That Will Replace Lawyers.* Retrieved from Blockgeeks: https://blockgeeks.com/guides/smart-contracts/

Saberhagen, N. v. (2013, October 17). *CryptoNote v 2.0.* Retrieved from Monero: https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf

CONTRIBUTORS

We would like to thank all of our amazing contributors who have made valuable contributions to the VSYNC project. We could not have done it without you.

THANK YOU

to the following:

Original Developers

Matt L.
Nicolas H.

Managers

Fishmaster 42
Pete S.

GitHub Contributors

VsyncCrypto
laanwj
gavinandresen
sipa
UdjinM6
non-github-
bitcoin
theuni
TheBlueMatt
presstab
luke-jr
vertoe
Fuzzbawls
jonspock
crowning-
Mrs-X
StakeBox
PIVX-Project
fanquake
gmaxwell
cozz
jtimon
petertodd
jonasschnelli
bit-bucks
snogcel
satoshinnakam
oto
muggenhor
rebroad
CodeShark
paveljanik
kdomanski
dooglus
schinzelh
super3
ENikS
wtogami
domob1812
dgenr8
morcos
scadding
wizeman
codler
jordanlewis
devrandom
joshtriplett
roques
sdaftuar
runeksvendsen
hellitonsm
dexX7
sje397
freewil
OttoAllmending
er
vegard
JoelKatz
jrmithdobbs
forrestv
dertin
p2k
schildbach
rdponticelli
21E14
Mkinney
Matoking
zw
celil-kj
mndrix
alexanderkjelda
as
fcicq
r000n
robbak
ashleyholman
4tar
federicobond
whitj00
mgiuca
elanaint
gjhiggins
roybadami
jayschwa
vsrinivas
mibe
globalcitizen
paraipan
grimd34th
brandondahler
gubatron
EricJ2190
jmcorgan
rnicoll
DomT4
sinetek
freynder
perrywoodin
mrbandrews
pstratem
thelazier
vinniefalco
al42and
ldenman

Website: www.vsync.io
Telegram: https://t.me/VSXcoin
Discord: https://discord.gg/Arqhyqg
Twitter: https://twitter.com/VsyncCrypto