



Lytix White Paper
Version 1.0, February 2019

Table of Contents

1 Introduction.....	3
1.1 Lytix.....	3
2 Lytix coin specs.....	4
3. Lytix economics.....	6
3.1 QuarkTX mining algorithm.....	6
3.2 Dash roots by way of PIVX.....	6
3.3 PrivateSend.....	7
3.4 Zerocoin.....	7
3.5 Lytix innovations.....	7
3.6 Development and release practices.....	8
4 Proof of Stake consensus.....	9
4.1 How to stake LYTX and zLYTX.....	9
5 Masternodes.....	10
5.1 How does the Masternode work?.....	10
5.2 SwiftX gift from PIVX.....	10
5.3 Lytix governance.....	10
5.4 Proposal voting.....	12
5.5 Masternode acquisition.....	12
6 zPoS protocol.....	14
6.1 Zerocoin technical details.....	14
A. Disclaimer.....	16

1 Introduction

There are countless cryptocurrency or cryptotoken projects in the market today. Each has their own flavor to meet the needs of a niche service. Lytix was born out of PivX, which forked from Dash, emanated from the original Bitcoin project. The Lytix team is committed to delivering a quality product that can fill the needs of different industries that require immutable transaction proof. Lytix also pulls in the private features of ZeroCoin to aid those that are not interested in publishing their transaction details to the entire world. Privacy is important, and this coin aims to enable that for all.

As you will notice, Lytix is not a coin like the others. First of all, and unlike most blockchain projects, the technology backbone came first. Then the purpose and the vision emerged. It's one of our many ways to be disruptive, in a sphere where disruption is key, and though it may seem like a negative point, we are trying the challenge of making it an advantage. We aim to create a platform to track transactions and provide proof of the transaction occurring. Our plan is to build on to the existing client APIs to enable descriptions and private functions within the transactions to benefit organizations and individuals a means of storing code or data within the blockchain itself. This will provide an immutable and assured environment for anyone to perform any form of transaction and have it saved for all time.

1.1 Lytix

Lytix (LYTX) is initially a proof of work coin. At first we thought about making Lytix a pool friendly coin, but as we moved forward it came to us that making it exclusively solo mined and CPU only would be the best way to make it accessible to everyone, and thus promote mass adoption.

By including CPU mining we aimed to have a coin that was available for all to mine and obtain. Some of the unfortunate events of the boom of Bitcoin led to a centralizing of mining pools and manufacturers. This was never the intention or dream of the original creators of Bitcoin. Our goal is to provide for decentralization by putting the power back into the individual miner's hands and to reward them after 5000 LYTX with the masternode system.

Masternodes are a critical part of Lytix and share the rewards with miners/stakers. As of this time the 30 LYTX reward is split between the two. Upon each new block, a masternode is randomly chosen and will receive the 15 LYTX reward.

Masternodes also have a critical role in voting for changes to the Lytix ecosystem. As the coin matures and the foundation develops we will use the voting system to provide changes to the foundation and

the coin itself.

2 Lytix coin specs

Maximum Coin Supply: 100,000,000 LYTX (will be lower due to fee burning + partial budget generation)

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

PoW phase	2-100,000
PoS phase	100,001-forever

Block size	2 MiB
Block time	60 seconds
Retarget time	1 block

PoS Stake Eligibility (requires wallet online and connected to network)

Minimum input age	60 blocks
Reward maturity delay	15 blocks

Transaction Send Eligibility

Minimum input age	6 blocks
-------------------	----------

SwiftX Eligibility

Locking delay	1 block
Spending delay	6 blocks
Collateral hold time	15 blocks

Privacy Technology

Protocol	Custom (based on libZeroCoin)
Accumulator modulus	RSA-2048

zLYTX denominations	1, 5, 10, 50, 100, 500, 1000, 5000
Mint time	≥0.5 seconds
Spend time	≥2.5 seconds
Maximum spend value	35,000 LYTX (can spend more)
Maximum spend denomination count	7
Mint fee	0.01 LYTX per zLYTX
Spend fee	None
Mint delay	6 blocks
Spend delay	20 blocks
Maturity delay	1:1 denomination mint added to accumulator

Proof of Work phase rewards breakdown

Block height Masternodes Miner

2-100,000 15 / 15

Proof of Stake phase rewards breakdown

Block Height - Masternodes / Staker

100,001 – 540,000 - 15 / 15

540,001 – 1,080,000 - 12 / 12

1,080,001 – 1,620,000 - 8 / 8

1,620,001 – 2,160,000 - 6 / 6

2,160,001 – 2,700,000 - 4 / 4

2,700,001 – 3,240,000 - 3 / 3

3,240,001 – forever - 2 / 2

As of this writing (Jan 2019) there is no governance or development fund with the exception of the 500,000 LYTX premine that will be used for initial development funding and expenses such as exchange listings, hosting services, and other small fees that come up in the course of running the project. All fees and charges will be documented and published on the lytixchain.org website to provide complete transparency of the effort. This will most likely change in the future and we will probably implement a small foundation fund on each block. This will be put forth to the members (holders of LYTX) for their buy in and agreement before being implemented.

3. Lytix economics

Lytix, as a clone of PIVX, burns its transaction fees as PIVX does. The platform is opened as a currency with decreasing rewards as blocks progress into the millions as described above to help offset inflation. The goal is eventually to become a token platform that can also be used as a currency.

Lytix now issues 30 LYTX into circulation every minute (15 for the miner or staker and 15 for the masternode owner)

There is a cap of 100,000,000 LYTX. Once that cap is reached there will be no more LYTX available for awards. This may be revisited some time if the hard cap becomes an issue. The idea was to have it high enough that the ecosystem could be flexible, but create some value with the cap. Rewards after block 100,000 will be through staking and through hosting the masternode network. Please see the schedule above for the rewards breakdown.

3.1 QuarkTX mining algorithm

In the PoW phase, Lytix utilizes the QuarkTX algorithm for its primary algorithm. QuarkTX is specific to Lytix but can be reproduced by any coin running Quark and ZeroCoin after the first block. Considering the needs of the community and a desire for a good CPU coin the decision was made to stick with the current algorithm and call it QuarkTX. This will move on after the PoS transition. Lytix will use the X11 algorithm moving forward after the PoS transition to be more energy efficient and not consume so many resources on the clients. The Quark was, however, shed with the shift to PoS.

3.2 Dash roots by way of PIVX

Dash is an altcoin focused on speed, and once focused on privacy. Dash is the direct predecessor of PIVX and Lytix. 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 decentralized nature of the masternodes will cause the market price to rise in response, limiting such efforts.

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.

3.3 PrivateSend

PrivateSend is a Dash feature that mixes coins to increase privacy. It does this to obscure some of the sources of the coins. This is designed to enhance privacy and Lytix pulled this in due to the attacks on privacy that we see everyday. We move the transaction to multiple transactions to increase privacy and make it more difficult to track the original transaction. We also pulled the masternode mixing into Lytix to allow multiple masternodes to split the transactions removing the single point of failure in previous versions.

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.

PIVX, too, utilized 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. Lytix has pulled in these features of PIVX's clone of release v3.1.1 of July 2018.

Lytix uses the same masternode system as Dash and PIVX speeding up the transaction times greatly. They work by consensus only allowing non-conflicting transactions into the blockchain.

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

3.4 Zerocoin

Lytix pulled zerocoin in to increase privacy even more than the original coin mixing strategy that Dash implemented some time ago. Zerocoin is a privacy centered coin that sits beside regular LYTX and can be minted after block 150,000. Minting zLYTX completely obscures the source and how it was created. You can send these coins, use them for purchase and the destinations and what they are used for will be private.

3.5 Lytix innovations

Lytix has similar feature to the coins it was cloned but aims to move forward with true API functionality allowing direct storage of other elements into the blockchain. It will be used as a currency or as secure storage platform for decisions that require immutability. The blockchain is a fantastic mechanism to provide this and Lytix aims to provide the security, stability and peace of mind that information will be immutable and never to be changed.

By the nature of the distributed network security and stability are almost a given. By using the coin as a means of payment as well as providing the reliability and immutability of the chain itself it allows enterprises to use the network as a decision storage matrix and for the miners and stakers to use the coin for purchases or for trading items of value.

Some potential use cases would be a financial services company that is undergoing regulatory pressure and needs a means of recording decisions about auditing tasks or completion of certain checklists. They could use the Lytix blockchain to record these decisions in an immutable storage system. This could also be used for chain of custody type situations where someone needs to prove that certain events or decisions occurred. Once they are entered into the blockchain they cannot be removed or altered.

With some of these use cases we plan to provide a Maxnode 2nd tier network that will house the APIs that the decision information will use to enter this into the blockchain. The maxnode system will cost 50,000 LYTX to house a node and participate in that network. They will also participate in the regular Lytix ecosystem and receive 10x the rewards that a regular masternode would earn. On top of the earnings from the Lytix network they will also collect fees from the API calls they receive to house information. This is undetermined at this point and the document will be updated later as the idea comes more into focus.

3.6 Development and release practices

Lytix is a project currently developed by the Lytix Chain team. Development is currently funded by the premine and out of pocket costs from the founder and lead developer. The goal will be for more people to join and changes to the platform will be approved by the community and the Lytix Chain team. We will try and utilize funding from voting for changes or dev funding utilizing the DAO governance system. As the premine is used to fund hosting, exchange fees, etc. it will be necessary to use the network to keep the network and development moving.

The Lytix Chain team utilizes a public GitHub repository to make updates allowing the entire community to see what is coming and what the particular impacts will be. It's important that there is complete transparency in code and the organization. All costs will be public as well.

The team also utilizes the standard Bitcoin testing utilized with Travis Code verification. No release will ever be allowed to fail testing. All changes are tracked, issues are documented, and all releases are on the GitHub site. The GitHub repository is the authoritative source for code, releases, and all documentation related to the code that supports the Lytix platform.

It is highly recommended that people and organizations use the latest stable release to mine/stake and participate in the network. It is possible to compile and run the code on your own, however non-released code may be marked as dirty or unknown and eventually banned from the Lytix network. Code consistency and stability is of vital importance to the Lytix Chain team and the future of the Lytix Foundation. The Lytix Chain team reserves the right to ban any node from the network that may cause issues or is running non-standard code.

4 Proof of Stake consensus

Like PIVX the Lytix network functions on a Proof of Stake consensus algorithm after the Proof of Work period will end at the 100,000th block. Staking will be active in the ZeroCoin zLYTX system at the 150,000th block.

Staking also uses computing power to process blocks and compete for stakes, but typically only runs at 1-4% CPU whereas mining would consume the entire CPU. Each node on the network competes for the right to insure the transaction and receive the stake. The higher the staking balance the more likely that the reward will be earned. The difficulty rises significantly depending on the amount that is in each block transaction.

If your wallet has 100,000 LYTX and is all being staked then you will be able to process transactions up to 100,000 LYTX. It is more likely that this wallet would receive the reward and insure the transactions than a wallet only containing 4000 LYTX.

Lytix decided to move forward with the Proof of Stake model after mining to also decrease the load on power and CPUs. It's a more stable system that consumes far less resources than mining.

Lytix enabled Proof of Work for a longer period to enable everyone to have a chance to obtain the funds prior to going on an exchange. We wanted to allow all people to have the opportunity to obtain the coins and not limit the availability to those that could financially afford it. The original thought was to allow PoW for 500,000 blocks but considering that the majority of the coin holders have already participated in mining and growth the number was brought down to 100,000.

Lytix, like its predecessor PIVX, is considerate of the demands that mining causes on the increase of electricity costs and the demand on electricity providers resources to provide electricity for the community and wants to enable a platform that is energy efficient.

4.1 How to stake LYTX and zLYTX

You can stake both LYTX and zLYTX on the Lytix network. Synchronize the wallet and at least have the minimum amount of coins that the network will accept. LYTX is 0.0000001 and zLYTX is 1 zLYTX. As stated above more is better in the staking world. You'll receive the reward based on the amount in the transaction, how much you are staking and also based on the random hashing mechanism built into the Proof of Stake algorithm.

5 Masternodes

The Lytix network is two-tiered and when the MAX nodes come online it will be a three tiered system. The staking tier is the first layer, then the masternode layer and finally the MAX node layer will provide the ultimate third tier.

Masternodes process transactions on the network and aid in speeding up the overall transaction processing. Unlike Bitcoin or other networks that are solely miner-based mechanisms masternodes help with privacy, transaction speed, and overall stability of the network itself. They enforce the PoS consensus mechanism to only allow consensus approved transactions into the blockchain.

5.1 How does the Masternode work?

They operate differently than staking nodes. Not one node has the power over the others and spreads out the work across all of the nodes in the system. Masternodes also have the right to vote on proposals for changes where stakers do not. This is discussed in more detail below.

5.2 SwiftX gift from PIVX

SwiftX is a pure innovation gift from PIVX and Lytix surely pulled it in due to the effectiveness and speed of transactions that it brings. SwiftX exists solely on the masternodes and decreases transactions times down to milliseconds. Whereas other networks can take hours to confirm transactions they happen at near real time because of the SwiftX protocol.

Masternodes work together to decide on how the transactions should be processed. When a transaction comes through one randomly selected masternode will lock the transaction. It locks it to just that transaction and will reject any other blocks or transactions for that SwiftX transaction. It will then broadcast the transaction through the ZeroMQ library. Once broadcast, consensus is achieved and it is instantly added to the blockchain.

5.3 Lytix governance

Lytix inherits the idea of a Decentralized Autonomous Organization (DAO), however the Lytix Chain

development team will also have a say in the future of the coin. The community and the masternode owners will have votes to help direct the coin and new features that are added to the ecosystem. The Lytix Chain development team will also participate in the system by owning masternodes and voting on measures. The amount of masternodes the development team may own will not be more than 10% of the total number of masternodes on mainnet. Each DAO has difficulties in proposal voting which is explained below. The majority of masternode owners tend to not exercise their right to vote. This leaves the coin system and the network hostage to apathy and inaction. To avoid these issues the Lytix Chain development community reserves the right to vote on enhancements and changes to the overall ecosystem in order for it to thrive.

We need to keep in mind that changes are not supposed to cause any harm to the system, on the contrary they are made to move the project forward, to stay competitive in the global markets and in the digital payments arena. The Lytix Chain development community will work hand-in-hand with the coin-holders and the masternode owners and hopefully we can avoid the stagnation and apathy that has hobbled similar efforts. Lytix 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 Lytix grows. This organic approach to governance is intended to draw the most value from members of the Lytix community, who themselves act in their own collective best interest.

Everyone in the community, including partners, coin holders, developers, and foundation members will have the opportunity to open proposals. Proposals will help us decide funding, direction, and addition of new features.

Masternode operators are granted the ability to vote on proposals made by community members with the intention of bettering Lytix, or circumstances for it, in some way. All members and coin-holders input is important. Ideas can come from anywhere and voting on proposals is an important step in defining where the Lytix coin will go in the future.

To ensure that the Lytix ecosystem flourishes and does not remain stagnant Foundation members, Enterprise partners, and Masternode owners will vote on proposals. The Foundation will act in the best interest of the community and will ensure that no one group holds sway over the coin or that the coin becomes stagnant. Control of the voting and the required amount of votes (percentage) is determined by the community. It's unlikely that we will get a majority of votes for proposals, because owners are busy and will not be able to put in the time required to vote.

To keep the ecosystem functional and moving forward we will break up ownership of masternodes and maxnodes to certain percentages to ensure that not one group has complete control of the ecosystem and dominates the decisions. Partners and corporate entities will be able to participate in the Max

node system as well as community members. To ensure that the network is not dominated by Max nodes there will be a cap and a cryptographic registration process required for registering a Max node.

Max nodes can not be more than 33% of the total Lytix ecosystem keeping in mind that each Max node is 10x a masternode. The foundation and development team will only operate a 34% max of the masternodes with the development team capped at 10%. 10% of the masternode proceeds from the foundation will go to charitable donations. The remaining 33% will be in the hands of coin holders and the community. It will be an attempt to keep the ecosystem flourishing while giving all interested parties a voice.

The enforcement details and technical details on how to achieve this will be forthcoming.

5.4 Proposal voting

Currently, the masternode network is responsible for voting on proposals that collectively determine the direction Lytix 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 decentralized voting mechanism set up in the rules governing the blockchain. This allows Lytix among other things to hire core developers and pay them directly after approval of the work in a decentralized 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.

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 Lytix Discord (discord.lytix.org). Here a proposal is introduced to active members of the Lytix community, with the general details being discussed, and members giving input based on initial impressions.

We are still in the process of formulating the official proposal process and this white paper will be updated when specifics are finalized.

5.5 Masternode acquisition

Operating a masternode on the Lytix masternode network is a very rewarding and somewhat technical task. We are working on the whole process to make it as user friendly as possible and as close to 'one click operation' as can be. There is no justification for the process to be accessible only to tech-aware people, so one of our goals will be to facilitate it. Each masternode owner has to have some level of skill involved and be able to maintain their own nodes and keep them up and available to participate in the rewards. Currently, masternodes receive half of the awards for each block.

5,000 LYTX is stored on the masternode controlling wallet. These LYTX must remain unspent as long as they are associated with a masternode wallet. This wallet should also be a distinct wallet from the one used to make transactions. Spending or moving in any way these LYTX will suspend the masternode status of the host wallet, thus revoking the eligibility for masternode rewards and the capacity to participate in voting. The necessity of these 5,000 LYTX serves several purposes, including ensuring a high enough percentage of staking nodes, and that the masternode host is likely to reliably provide a masternode service for the network over time, rather than simply dabbling.

Each masternode instance requires a 5,000 LYTX investment and needs to be reachable from a static IPv4 or IPv6 address. Our innovative membership has found a process to have multiple masternodes on a single instance. We love innovation and applaud the ingenuity, especially since this innovation works in the direction of a more sustainable and environment-friendly network. Each masternode needs to have its own alias, key, transaction ID (transaction showing the investment), and listen on its own RPC Port.

Our masternode guide is located on the main website at

<https://www.lytixchain.org/guides/masternode.html>

Our ingenious masternode virtual how to is currently stored at

<https://www.lytixchain.org/guides/mnhack.txt>

You may run a masternode on any platform as long as the above has been secured. We have masternodes on many different platforms and applaud the diversity and technical know-how of our coin-holders.

5.6 MAX node system

The Max node system is unique to Lytix. Max nodes will hold the APIs that entities will be able to use to store data into the blockchain. They will cost 50,000 LYTX each and will also receive 10x of the rewards that masternodes receive. They will be the only points of entry to the data storage and decision matrix with the Lytix blockchain. Max nodes are unique and identified by a cryptographic

signature that will tie it to the clients that own and use that Max node. Max nodes can also be private and the information stored and the decisions tracked can also be private. If the entries are deemed private they will be signed with the cryptographic signature and encrypted before placement into the blockchain. Only key holders that are part of that group will be able to view and decrypt that information.

We will expand more on this system and update this section as development is closer to release for this portion.

6 zPoS protocol

zPoS is Lytix's private Proof of Stake protocol based on Zerocoin and inherited from PIVX. Coin holders can remain anonymous while staking using zPoS.

Coin holders staking zLYTX receive 50% more rewards to try and interests coin holders in staking their zLYTX. It increases the privacy of the coins and helps keep those transactions and the origination of those coins.

Staking zLYTX just requires a balance as described above and having the wallet online and unlocked. This period will start after block 150,000.

6.1 Zerocoin technical details

Lytix Zerocoin protocol Technical Specs (v2.0)

Key Features: Custom accumulator checkpointing system

zLYTX version 1 Phase Period: block 150,001

zLYTX version 2 Phase Period: block 500,001

zPoS Phase Period: block 150,001

Accumulator Modulus: RSA-2048

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

Mint time: ≥ 0.5 seconds

Spend time: \geq 2.5 seconds

Maximum single Spend limit: 35,000 LYTX

Maximum single Spend denomination count limit: 7

Block size: 2 MB

Fees (mint): 0.01 LYTX per minted zLYTX denomination.

Fees (spend): No fee to spend zLYTX back to LYTX.

Minimum LYTX confirmation count required to mint zLYTX: 6

Minimum zLYTX confirmation count required before spend: 20

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

Confirms before zLYTX can be staked again: 200.

A. Disclaimer

You are viewing a version of the whitepaper from February 26, 2019. Our business, legal frameworks, and technical teams and direction may change in the future. Lytix is an experimental cryptocurrency project. Also note that Lytix is not a currency backed by any government, financial institution, or other legal entity. Lytix is not recognized as a legal tender or any sort of legal entity.

There is some risk in trading cryptocurrencies. Lytix, The LytixChain Foundation, or its creators are not responsible for any loss incurred when trading or transacting using Lytix as a currency if the owner chooses to use it as such. The information presented here is general in nature and can change at any time. The Lytix Core team and the LytixChain Foundation reserve the right to change this document or the technical direction at any time without prior notification.

Please do your own research before investing or owning cryptocurrencies and would be best advised by a certified financial planner to understand all of the risks involved. The Lytix Core team, the LytixChain Foundation, or it's contributors to the open source code are not responsible for any damages from using Lytix inappropriately or using Lytix at an exchange. The Lytix Core team has made every effort to ensure that all of the information contained within this document is accurate and current. The information provided in this whitepaper is "as is" without any warranty. The Lytix Team does not accept any liability or responsibility for the completeness of the information provided. We have made the best effort to assure its accuracy. The Lytix Core team, the LytixChain Foundation, and our open source contributors are not liable for any damages or loss of any kind of any loss, damages, legal disputes, contract issues, or malfeasance as a result of any action that occurs from obtaining or investing in Lytix.