# ENOX

## WHITEPAPER v1.0

https://enox.io

# TABLE OF CONTENTS

# WHAT IS ENOX?

Enox was born from choosing and forking PIVX for being one of the best privacy coins out there. Enox is a new digital online money with the technology of blockchain and masternode.

Cryptocurrency that incentivised coin holders with the idea of the MasterNode (MN). The MN operator helps to validate the super fast transactions (InstantPay) and provides the anonymity for the coins on the network.

Cryptocurrencies and blockchain technologies have given rise to new ideas and innovations that have reshaped the global financial landscape. Connecting people and resources in a speed never seen before, peer-to-peer decentralized networks have empowered citizens with the ability to exchange payment for goods and services without relying on traditional banking, FIAT currency, or creditors. A truly free society is being developed with instant, private transactions emboldened by the promise of blockchain technologies. Although Bitcoin has been the catalyst for this new movement, it lacks some key attributes that have been improved upon in several new cryptocurrencies. Our mission is to blend several of these elements to introduce the fastest, privacy-based coin with a network of Masternodes (MNs) for security.

The cryptocurrency space has seen a plethora of innovations to address multiple issues that have arisen since the inception of the first blockchain based protocol, Bitcoin. Controversy regarding miner centralization and practical issues such as fungibility and privacy have been addressed. As the network grows, security becomes less of a factor while getting a consensus vote for implementing changes becomes increasingly di icult. The form of a voting system via MNs allows for a distributed group to vote on a continuous basis on matters pertaining to ENOX without giving up their right to vote to others. It is the community who will choose which problems ENOX seeks to solve as we move forwards in harmony with the ever changing blockchain environment.
As such, ENOX begins its journey by forking from the Pivx repository, a cryptocurrency based off Bitcoin's core 0.10x code base and running Blackcoin's Proof of Stake (PoS) 3.0 protocols. Maintaining the stable core code whilst adding the addition of MNs which will give resources for adding additional features such as governance, privacy, and faster transactions. Communities and the internet have been synonymous since the first message boards sprang up in the 1970's. Now with the advent of cryptographically verifiable digital ledgers it has be- come possible for these communities to exchange value digitally, securely, and quickly.


## THE FIRST TO OFFER A CHANGE

The legacy of Bitcoin will always be established in the fact that it was first to publish this amazing new technology. A pioneer of its time, the solutions that the cryptocurrency offered are revolu- tionary. Allowing buyers and sellers to create commerce without a trusted third party to conduct their transaction. Changing the dynamic of conventional payment systems from a trust-based model to one that requires cryptographic proof begins to elimi- nate fraud and corruption. Timestamps provide chronological or- der of transactions, while digital signatures verify them and their contents.

Nodes are an integral part of the blockchain network. Not only do they verify transactions but they also verify the outputs of other nodes, thus maintaining the networks integrity. As the digital ledger continues to grow, so does the memory require- ments to store it. As such, lite nodes serve to function on small memory devices such as phones which contain only the parts of the blockchain that they require. They then query a full node for verifiability. Full nodes refer to nodes with the complete block- chain on it, yet in some cases this does not need to be the case.

Bitcoin utilizes a 1 tier incentive structure to secure its network. M iners operating full nodes are also able to spend computational and electrical power in tacking another block to the blockchain, thus confirming all the transactions sent by the nodes. This pro- cess mints a new coin rewarding the miners for their contribution to the network.


## MASTERNODING THE CHALLENGES

Looking to reward full nodes, Dash introduced a second tier to their system known as Masternodes (MNs) in 2014. This second tier allowed for additional features such as privacy and faster transactions to be performed on the network with MNs being incentivized by receiving a portion of the block reward for per- forming these tasks.
While in a 1 tier system, only the miners are incentivized to com- mitting computational and electrical power to securing the net- work. In a sense, they are voting for code changes in the form of updating their node software. In a 2-tier system such as Enox, its incentive structure is split between MNs and traditional (PoS) stakingwallets.MNsrequire10,000Enoxcollateralandamini- mum downtime of 1 hour per day connectivity. They receive 65% of the block reward for their contribution. The remaining 35% of the block reward goes to traditional staking wallets. These two tiers are treated different when it comes to incentives, based on resources needed to participate.
This type of structure allows rewarding network participants based on their contribution of resources to the network, while at the same time sets an inherent cap based on diminishing returns. Meaning, if too many MNs are built, the remaining 35% of the reward becomes greater if 10,000 Enox is staked rather than being used to build a MN.
Masternodes facilitated by the PoS 3.0 framework offer a more robust network to build upon making the incorporation of other features easier; be it governance, privacy, security, or further decentralizing the network. MNs at present only facilitate vot- ing and are intended to allow advancement of the project in the future. This network structure allows Enox to implement ad- ditional features to keep up with development as well as imple- menting additional features should the community vote in favor of them.

## FASTER TRANSACTIONS (sWIFTX)

Another benefit of utilizing this form of network is that users can send and receive instant, irreversible transactions. Once the MNs reach consensus on a transaction, the inputs of that transaction become locked and become non-transferable else- where on the network. The process takes about four seconds and is a decentral- ized means in allowing near instant payment for real world commerce as well as peer-to-peer exchanges.

## GOVERNANCE

Governance takes the form of nodes/users submitting propositions which are vot- ed on by M N holders each super block (approx. 1 month). M N holders either reject or accept submissions regarding changes in protocol, brand or, direction of the project. Developers retain the right to veto any change that is technically not pos- sible or if the technical solution is alternate to the proposed statement voted on.

## ZEROCOIN

Pivx was the first PoS cryptocurrency to use and improve upon the Zerocoin public repository. Pivx is a protocol created by academic cryptographers that allows users on the network to interact with zero knowledge proofs, thus minimizing the amount of data transmitted with a transac- tion. This protocol protects both the sender and receiver by only sharing information pertaining to the amount that was sent, known as the value.

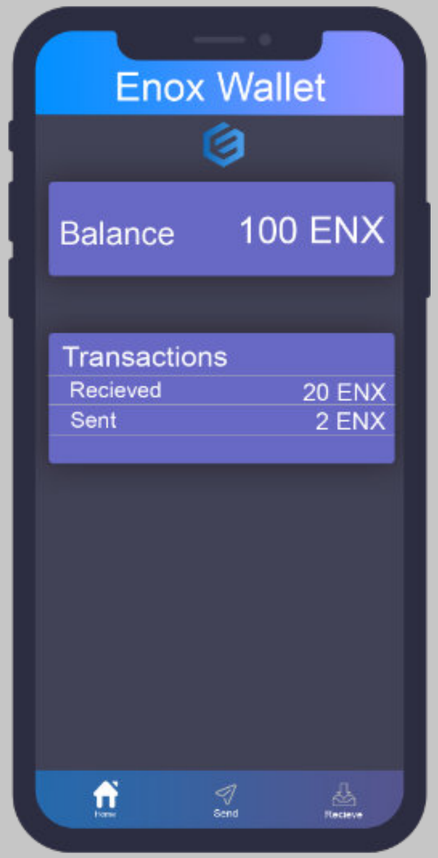
Users of the Enox network can choose to convert their normal Enox (Enx) coins into a denominated amount of zEnx coins, thus dissociating any of their wallet information from the transaction ID. This allows for a verifiable asset transfer to occur anonymously through the network.

Zerocoin protocol functions by “burning” the zEnx transac- tions at these denominated values with other user’s trans- actions. A zero-knowledge proof is then executed to mint new coins that are sent to the correct addresses. The pro- cess is quick and respects both the privacy of the sender and receiver as well as removing any unwanted histories associated with the received coin.

The benefits of privacy in cryptocurrencies are that they become fungible and safer to use. This protects the com- munity’s balances from prying eyes whilst still maintaining the option to send a fully transparent transaction, should one be required.

# MOBILE PROOF OF STAKE

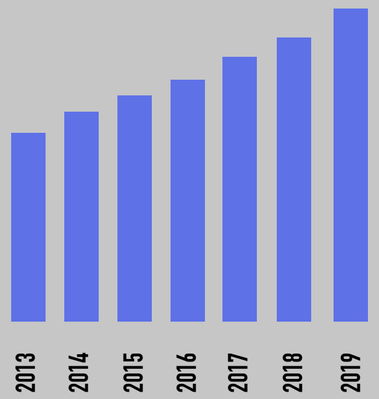





## INTRODUCTION

Technology never stop, ideas never gets behind we are proud to introduce you our enox mobile staking a real crypto game changer, it is the old proof of stake ( POS ) idea but injected on your mobile devices, We all know how sensitive POs is, we need Computers/VPS running in order to stake a coin. That`s just not cool anymore, so that being said, yes we want to have MobileStakingWallets, fully decentralized, full node continuously syncing and providing actual security and validation on the enox blockchain. Team is about to create a tiny tool with a giant features that would take lesser computing efforts to make sure it was secure and fully funcional. The world will adopt cryptocurrency, enox will be the gateway for those people more on mobiles that want income without investing on expensive rigs.

Mobile staking idea is to bring more people into the crypto space as we all know computer users are outnumbered by mobile users. Let the app runs in background and start staking enx coins.




## THE MASS ADOPTION

The total number of mobile phone users worldwide from 2013 to 2019. For 2017 the number of mobile phone users is forecast to reach 4.77 billion.

The number of mobile phone users in the world is expected to pass the five billion mark by 2019. In 2016, an estimated 62.9 percent of the population worldwide already owned a mobile phone. The mobile phone penetration is forecasted to continue to grow, rounding up to 67 percent by 2019. China was predicted to have just over 1.4 billion mobile connections in 2017, while India was forecast to reach over one billion. By 2019, China is expected to reach almost 1.5 billion mobile connections and India almost 1.1 billion.

Most of the mobile market growth can be attributed to the increasing popularity of smartphones. By 2014, around 38 percent of all mobile users were smartphone users. By 2018, this number is expected to reach over 50 percent. The number of smartphone users worldwide is expected to grow by one billion in a time span of five years, which means the number of smartphone users in the world is expected to reach 2.7 billion by 2019. Samsung and Apple are leading smartphone vendors, with about 18 percent of the market share each.

Enox biggest mission is to provide the world a better experience in crypto, with its mobile platform we are challenged to hit the mass adoption. We are not just gaining peoples for numbers, we are gaining people to have a real change on their crypto vision.

The mobile POS app is a tool for people more on mobile, that works just like a credit/debit card. 3rd country nations has difficulties to have a bank account, personal computers, lets just forget about those, with the app just using your mobile phone you have all the tools.

# MOBILE PROOF OF STAKE



## APP FEATURES

Aside from having the proof of stake integrated on the app, it also comes with great features.

### SECURITY

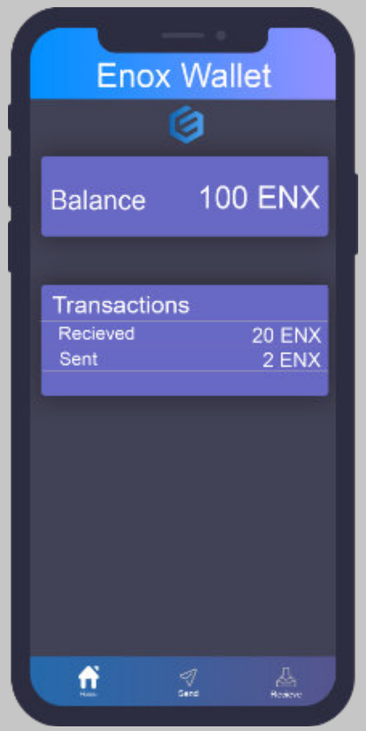
Multi-factor authentication is essential for any enterprise app that stores, processes or accesses sensitive corporate data or personally identifiable information.

MULTI FACTOR AUTHENTICATION WITH BIOMETRICS

COMMUNICATION ENGINE

REMITTANCES, BILL PAYMENTS, MERCHANT PAYMENTS

VOUCHER MANAGEMENT, INVENTORY MANAGEMENT




IN BUILT TEAM WALLET

COINCARD IMPORT/EXPORT

CARD ISSUANCE LINK TO WALLET

NFC AND QR PAYMENTS

### UTILITY

Your staked rewards will have an option to be seperated on your staking balance and can be used to pay for your bills, such as carrier bills payable directly from the app,remitances etc..

# ROADMAP

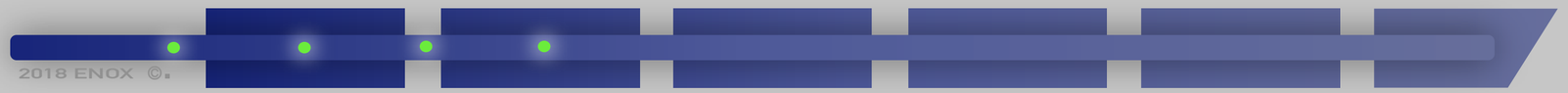
**In depth guide of enox´s journey. A real challenging and exciting year to come.**

## Q2

CORE DEVELOPMENT
MULTI WALLET RELEASES
WEBSITE DEPLOYMENT
MOBILE POS DEVELOPMENT

## Q4

MARKETING CAMPAIGN
MOBILE WALLET ADDED FEATURES
NEW DESKTOP WALLET GUI
EXCHANGES LISTINGS




## Q3

MNO LISTING
STOCK.EXCHANGE LISTING
MOBILE POS PHASE 1 TEST
MOBILE POS BETA TESTERS

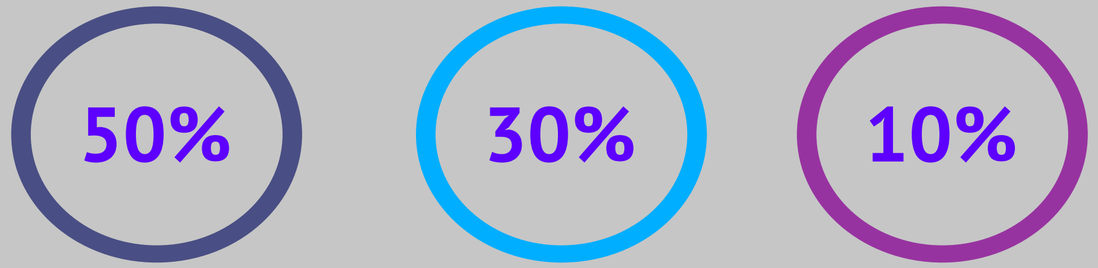
## Q1

MOBILE CARRIER PAYMENTS
MOBILE POS v2
2019 WHITEPAPER RELEASE
EXCHANGES LISTINGS

## COIN DISTRIBUTION

Premined coin are distributed as such.

### A TOTAL OF 450,000 WERE PREMINED




- 300,000 ENX WILL BE AVAILABLE FOR MASTERNODE PRESALE FOR THE MPOS PROJECT AND COIN LISTINGS.
- 100,000 ENX WILL BE AVAILABLE FOR AIRDROP FROM OUR OFFICIAL GOOGLE FORM.
- 50,000 ENX WILL BE AVAILABLE FOR BOUNTIES AND GIVEAWAYS.

## COIN SPECIFICATIONS

**Algo :** Quark

**Block Time :** 60 Seconds

**Difficulty Retargeting :** Every Block

**Max Coin Supply (PoS Phase) :** Infinite

**Premine :** 450,000 ENX

**Masternode Collateral :** 10,000 ENX

**Port Collateral :** 21001

**RPCPort Collateral :** 21002

**Written using the Quark algorithm speed per block: 60 Seconds**
**This is a full proof of stake coin.**

## REWARD SYSTEM

MASTERNODE HOLDERS HAS 65% SHARES FROM THE REWARDS.

STAKE RSHAS 35% SHARES FROM THE REWARDS.

| Block Height | Reward | Masternodes | Stakers |
|---|---|---|---|
| <= 755,600 | 10 ENX | 6.5 ENX | 3.5 ENX |
| 755,601-1,043,999 | 5 ENX | 3.25 ENX | 1.75 ENX |
| 1,044,000-1,562,398. | 2 ENX | 1.3 ENX | 0.7 ENX |
| => 1,562,399 | 1 ENX | 0.65 ENX | 0.35 ENX |

# THE TEAM



**JUNNY MING**
CEO/C#

**LIAM WARD**
BLOCKCHAIN/POS/C#

**MARKSON YUAL**
MOBILE DEV/C#

**ALEX FRED**
MARKETING

**ANNE SUE**
COMMUNITY MANAGER

**JENNY LUE**
MARKETING

**SV-TECHNIL SASCHA**
ADVISOR

## INTRODUCTION

Cryptography has managed to change the way finance and money is defined. Recently the advent of Bitcoin[1] has showed how a peer-to-peer network can prevent forgery by solving the "Byzantine Generals Problem." Since then many different coins have been created based on Bitcoin's open source code. There are two major methods for generating new funds on the network. The first is "Proof of Work" and the second being "Proof of Stake". The theory behind Proof of Work is to hold a mathematical competition. The first computer to solve the puzzle receives the coins. This makes distribution of coins a completely fair process. However, this also creates a problem of wasted energy. Computers in order to compete, create and arms race of hardware. Thus, money and energy is wasted to generate new coins. Proof of Stake is a competition between shareholders, where based on connectivity to the network and random chance, you can receive new coins. Interest is generated based on how much you hold. This solves the energy waste problem in Bitcoin and introduces new challenges in network security. Here at Blackcoin, we would like to write a technical analysis of the advantages in this protocol and to honor our predecessors, discuss potential improvements and pitfalls. Proof of Stake was first implemented in "Peercoin"[2]. Later, major breakthroughs in Proof of Stake were made in Blackcoin namely, "Proof of Stake 2.0"[3] and "Proof of Stake 3.0". We have implemented the Proof of Stake 3.0 system because we believe it to be the worlds most secure and efficient method of coin generation. We will outline and highlight the great security of this system and the technical problem it solved.

## Security, Coinage and Attacks

The whole purpose of holding competitions for coins is to avoid attacks. Confirmation of transactions is an honor given to the winner of a block. However, if this system can be gamed, then it is flawed. In Proof of Stake, you first prove you have access to coins and from that point you can compete to win blocks randomly. The more people competing the more secure the block. Coin age is the idea that the longer you hold coins the higher the probability you can win a block. It's original intention was to incentive dormant holders of coins. However, this does not encourage a node to stay connected to the network in practice since they can wait for the reward to increase. Also, shareholders can disconnect from the network for long periods of time, then reconnect and win enough blocks to risk a 50% attack on the network. The time calculation will effect payouts discouraging connectivity. Also, the fewer the nodes that are connected, the easier it is to gain a majority of the blocks forging consensus. Also, stakes can be computed in advance to make the attack more effective. Timestamps are used in Proof of Stake to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps. In Proof of Work, a difficulty increase or decrease is made depending on how quickly a block was produced. However, as a precautionary method to prevent any sort of "Timing Attacks" Proof of Stake coins use centralized checkpoints.

Coin Age

Coin Age is calculated by the weight of unspent coin and the time they have been dormant. The calculation is simply "proofhash < coins · age · target"

The proof hash is the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. The attack of saving up Coinage was previously outlined as improbable[3]. The reasoning behind this is because it is very difficult to perform consecutive double spending since Coin-Age would reset after the first expense. However, this is not entirely clear because an input can be split into 1000s of outputs. This may give the possibility for consecutive double spend attacks. However, this is still a difficult problem because the attacker would need a significant amount of funds to hold weight greater than the network. In theory, this makes sense. However, if we look at the amount of forks of Blackcoin and other popular POS systems, we can see the amount of nodes are fairly low and this gives much greater weight to a smaller handful of nodes. A holder of many coins may not want to perform this attack since they run the potential of losing value of their share if detected. However rational this may seem, it is probably a fallacy because it is still an attack vector and a very real one indeed. More importantly, with so many coins being published daily, keeping as many nodes connected as possible is imperative to security. Solution from Proof of Stake 2.0: Remove Coinage from the equation - "proofhash < coins · target".

## Security, Coinage and Attacks

Blockchain Pre computation

The block timestamp is key to the Proof of Stake system. It is possible in theory to fork a coin by changing previous timestamps. The stake modifier does not obfuscate the hash of sufficiently to prevent knowing future proofs. So an attacker can attempt to compute all of the blocks in advance and run a higher probability to forge multiple consecutive blocks. Solution from Proof of Stake 2.0: The stake modifier is changed at every modifier interval to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake. The expected block time was increased from original 60 seconds to match the granularity.

Past limit: Time of last block

Future limit: +15 seconds

Granularity: 16 seconds (effectively increased from 1 second)

Expected block time: 64 seconds

Block Reward

The Block Reward in most Proof of Stake systems is unfortunately based on Coin Age. In theory, this is to distribute interest fairly by allowing nodes to receive latent payments due. It is an attempt to keep a common APR. However, this system does not work because nodes can stay disconnected and with many split inputs, reconnect to the network and game the reward system. Also, it does not give nodes any incentive to stay connected. In a decentralized system, the more nodes connected the better the security since it shifts trust from a single entity to the network itself. Solution from Proof of Stake 3.0: The block reward was made a constant 1.5 coins per block. This was based proportional to the supply of coins maintaining interest at %1.

## MULTISIGNATURE/COLD STAKING

The final noteworthy addition to the protocol was the implementation of "Multisignature Staking". One drawback to many staking algorithms is they only support staking with a single key. Since the popularity and use of software such as BlackHalo[4], which uses a two party escrow system also known as "Double deposit escrow" and more secure dual key accounts, it has become important to allow these accounts to participate in securing the network. Beyond dual key accounts there is many other types of inputs that make use of p2sh and lock times and those must also be allowed to secure the network as well. The other problem is that in a single key account, a hacker can use key loggers to obtain your password and compromise your wallet while it is unlocked for staking. Solution from Proof of Stake 3.0: We allow users to place the block signing key in the output of "6a" known as a burn address so they can stake by sending a standard transaction. This allows any input to be eligible for submission. This gives Blackcoin a huge advantage for custom staking software, voting and the legendary "Cold Staking". The "Cold Staking" technique involves multiple computers. Basically when a multisignature input is eligible for staking, the signatures are split up between many computers. This makes an account virtually impossible to hack because even if a single key was compromised, the other keys are in a completely different location either on the local area network or on multiple servers. This technology is already being implemented in the latest release of BlackHalo.

## SECURITY ANALYSIS

The elimination of Block Reward based on time was an obvious improvement. Thus, if the amount of nodes staking drops, yearly interest would increase proportional to the disconnected nodes. For example, if only 1/5th the network was Staking, you can expect up to 5 times the reward! Since many coins do not have enough nodes, this is a great advantage even to smaller shareholders. Although statistical data on all relevant coins would be time consuming to obtain, it is self-evident that there is usually a lot less than 20% of the shareholders staking. We think this increase in incentive will certainly keep the nodes more competitive. The change in granularity was useful to prevent "Stake Grinding". A good analysis of the probability of this attack was done in Neucoin[5]. Their claim is that even with all the hashing power of the Bitcoin network, the attack would not be possible. However, a rollback of a few minutes could cause new users to the network unsure of which chain to join. Therefore, Proof of Stake systems use "Checkpointing" which is basically centralized control of the main developer to choose chains that attempt to do this. Of course, this is not an ideal solution. There was a good proposal made in Ethereum[6] for this. They proposed that a new node to the network asks other nodes "off-band" if they are indeed on the correct chain. Using our decentralized markets, it is possible we can get nodes to share this information periodically. The solution will require further investigation.

# RESOURCES



| | |
|---|---|
| **Bitcointalk** | https://bitcointalk.org/index.php?topic=3454998 |
| **Telegram** | https://t.me/joinchat/HjWVsQ6h7IefDUDRGV9JBA |
| **Discord** | https://discord.gg/xKznxDq |
| **Twitter** | https://twitter.com/EnoxMasternode |
| **Website** | https://enox.io |