NIX Platform whitepaper v1.0

April 30, 2018

NIX

Table of contents

1. The Emergence of a Data Revolution

Blockchain protocol has revolutionized the way the world looks at data storage mechanisms. Specifically, P2P networking helps achieve this decentralized distributed consensus by combining the advantageous appliances of blockchain and P2P design. With that, a new era of data management and financial asset storage sprouted and came to life. With the creation of the first blockchain digital currency, Bitcoin, in early 2009, many researchers and like-minded visionaries recognized the potential of independence that this technology holds.

With the concept of centralized organizations controlling operations from digital commerce to financial industries, it is evident that in a world of growing and ambitious individuals, these types of organizations hold threat to the advancement of both the world and the way social structures are molded.

Throughout history, it is seen that all centralized entities have their downfall as social structures advance and humanity progresses. Leaving the power held to a select few to determine the future of evolvement of humanity is the exact reason why blockchain P2P networking was created.

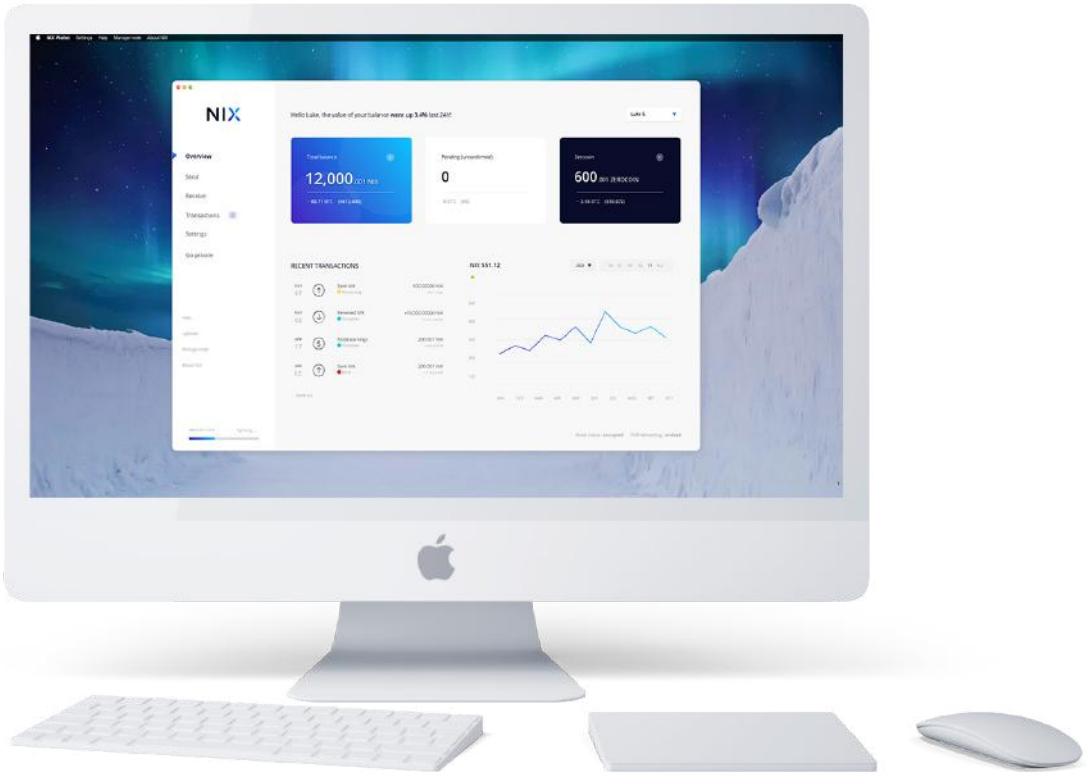
.

2. Objectives and Purpose

NIX aims to grant the means and resources that will empower people across the world to achieve independence in their social, economic, and global structure. These assets span from financial security and freedom to private data management and even social content autonomy.

The key issue within the blockchain and cryptocurrency realm in the present is user integration. Although the technology has been battle hardened to an extent, real world development and use case is little to none. The adversity that NIX aims to solve is bridging that problem and empowering elements to create ecosystems with a specific use case. In order to achieve this, NIX will adopt multiple privacy mechanisms, scaling solutions, smart contracts integration, sidechain utilities, and ease of use towards the end consumer specifically in speed and environment.

The NIX protocol will offer layered optional privacy that will enable people to create a medium of communication and dApp's between blockchain channels, for whichever purposes each channel stores.



3. Initial Use Case Adoption: Private Decentralized Trading

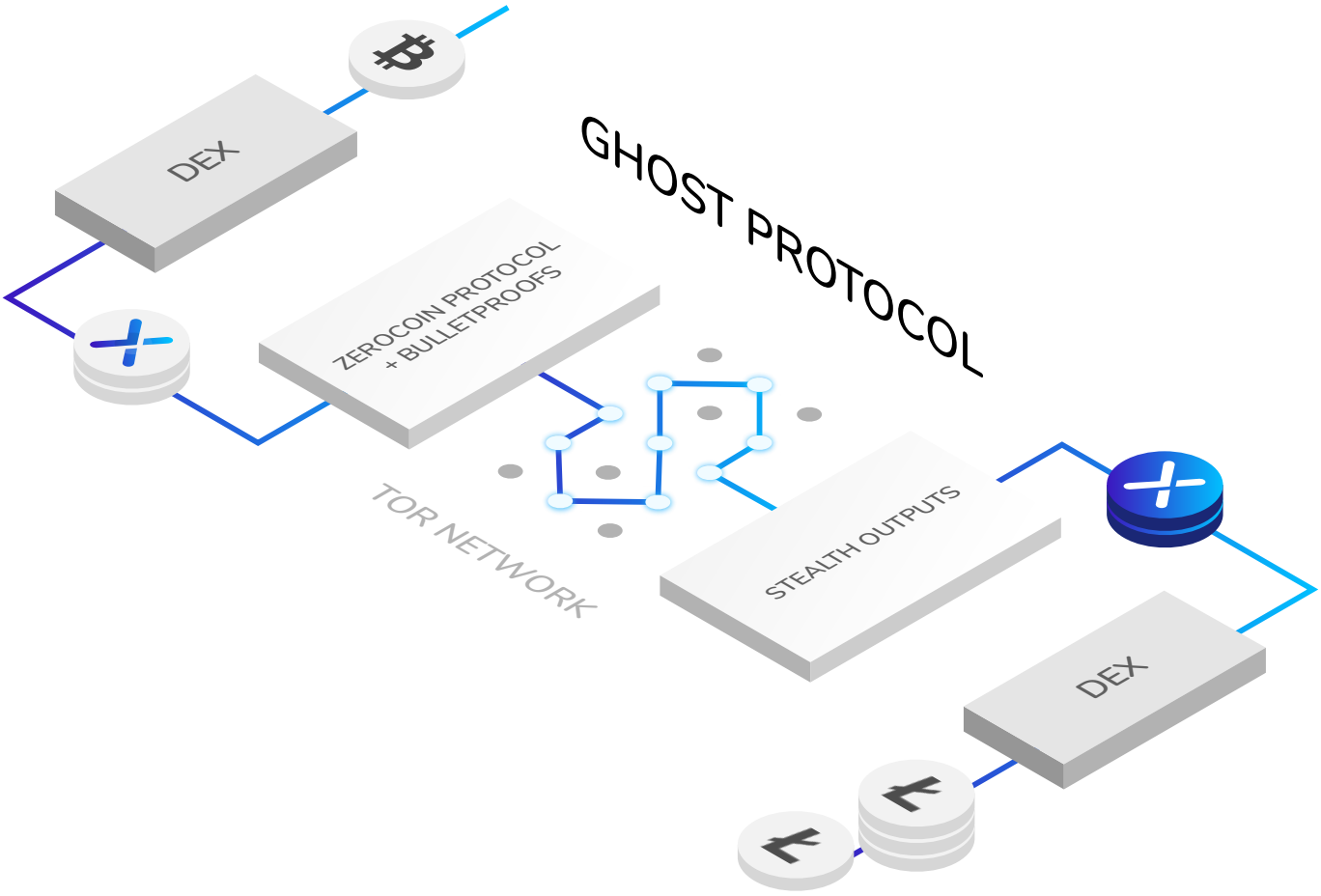
To demonstrate an important aspect for the financial world in cryptocurrency, NIX is targeting the creation of the first privatized decentralized exchange initially through the usage of the Blocknet protocol. This system will be designed to solve privacy layers among DEX trading, creating a layer of privacy for any protocol and tradeable asset through a multi-tiered trading structure. NIX will bridge communication within external DEX's to create privacy elements among all and any compatible ecosystems. NIX has partnered with Blocknet to achieve this system unification, permitting direct development on each protocol in a streamlined fashion as a prompter integration is developed.

NIX, with the integration of the Blocknet network, will allow for the exchange of one cryptocurrency for another without the need of a trusted third party. On traditional markets, a trusted third party is required for users and traders to engage and trade currencies through an escrow. Many times throughout the evolution of cryptocurrency trading, this trust has been abused and traders/users have been taken advantage of. The use of atomic swaps eliminates this issue, and the process for a NIX privacy swap is simple.

To trade coin A for coin B via the NIX platform, there are several steps that take place to ensure that when a trader receives coin B, the swap is untraceable and private. The privacy process to swap coin A for coin B works on both routes: Coin A and B are mutually traded for NIX. Please note that this is possible with any decentralized exchange protocol, yet the initial and the one taken as primary reference in this paper will be Blocknet DEX.

NIX Ghost Protocol transactions are conducted by means of the NIX Ghost Nodes (NIX Coins) ensuring an anonymous and private trade. Once the coins are privatized and become untraceable on the network to their origin, they are in turn traded for Coin A and Coin B and sent to the respective traders. Finally, the initial Coin A owner holds Coin B amount

which was generated from the Zerocoin anonymous transaction that the NIX network created. Same for the Coin B owner. All coins are then traced back to the NIX trade that it used, and since the NIX coins hold no prior record, there is no historical trace of the atomic swap creating a privacy layer for atomic transactions.



1. Technical Elements

NIX is being built to establish an ecosystem of asset distribution with the added power of privacy centered metrics. To achieve this, the initial design regarding privacy targets several user adoption elements. NIX has created a unique, personal privacy library, named the NIX Ghost Protocol, that will use the mechanisms of Zerocoin privacy proofs and Bulletproof layers, paired with one-time integrated Zerocoin addresses. This will then be combined with a Tor network that offers OBSF4 bridging and communication. All elements from networking privacy to blockchain privacy will be offered.

This layer of privacy focuses on both chain-to-chain asset control as well as intra NIX chain usability.

2. Inter-Communication Model

The creation of an inter-communication model within the NIX environment points multiple elements. The utilization of privacy centered smart contracts will allow for dApp's to fill the space for chain-to-chain communication protocols. The first case of a dApp in creation to NIX's ecosystem will be the bridge between DEX platforms in delivering a privacy layered system to privatize atomic swaps.

Branching outwards, the NIX architecture will allow the creation of any chain-to-chain communication layer to use the privacy metrics that NIX offers. Not only will NIX provide value in its own financial ecosystem, it will also consent utility in a smart contract privacy system. To enable creation of chain-to-chain mechanisms, NIX will allow users to lock the network required consensus for a chain-to-chain creation. Essentially, when a user wishes to create a dApp that operates within the NIX dominion, the initial fee for allowing creation on the

platform will entitle users to deposit NIX into a network distributed address, this address fulfills agreement requirements in the establishment of the communication model.

On the NIX network, there will be specific NIX Ghost Nodes that work to accomplish these consensus requirements. For example, the Blocknet DEX communication model will be handled between NIX Ghost Nodes on the NIX network. With the NIX consensus system utilizing proof-of-work on chain, NIX Ghost Nodes will be used to approve and fulfill cross chain protocols. The use of NIX Ghost Nodes will generate an automation of network privacy for these created ecosystems.

3. Intra-Communication Model

NIX will not only offer privacy to outside entities, but will also create superior privacy elements for NIX data distribution.

4. Sidechain Model

The integration of a sidechain ecosystem in NIX offers users, developers, and businesses the opportunity to create and attach their own networks to the NIX network. The purpose that sidechains aim to achieve within NIX is to create a framework that will allow network customization without requiring a change in the NIX core protocol. This will play a big role in NIX's direction at solving supply chain management through blockchain.

5. NIX Ghost Nodes

NIX Ghost Nodes will be created to help ensure dedicated network processing for Ghost

Protocol transactions. Any smart contract based element that requires autonomous privacy processing will rely on the NIX Ghost Nodes to fulfill that request. Maintaining and running a NIX Ghost Node is a completely decentralized process in which a user needs to obtain 40,000 NIX coins to run. By staking these NIX coins, the network will use nodes to dedicate power for NIX Ghost Protocol transactions ensuring no bottleneck in the computing component of each privacy element; in return, each Ghost Node is rewarded as follows: a.) there will be a 0.25% fee rewarded to NIX Ghost Nodes through any Ghost Protocol transactions enabled by smart contract elements, which is a small charge to pay for decentralized privacy that also includes atomic swaps. A small charge to pay for decentralized privacy. And b.), NIX Ghost Nodes will additionally earn partial block rewards of 28% per block.

6. Optional NIX Ghost Protocol Privacy Model

The superior privacy layer that NIX offers solves many concerns in the cryptocurrency ecosystem. Because NIX believes that users should have the power of privacy, it is not a required feature, simply an optional one.

With Zero knowledge proof elements for concealing transaction and data movements along with one-time addresses to protect the location of users, the NIX privacy protocol is the most robust and mathematically secure system.

The construction of the privacy mechanism follows that of a slightly modified Zerocoin setup still utilizing the RSA and Discrete Logarithm system for a zero-knowledge proof setup. For the Zerocoin parameter generation, NIX creates a scheme that has 4 checkpoints. The initial layout is the Setup parameter, followed by Mint, Spend, and finally Verification. The two factors that are modified for the construction of the NIX model focus on the last two elements, Spend and Verification.

[1]Value not yet determined

Initially, a setup parameter is designed in order to create an accumulator environment with prime numbers p and q such that p = 2q. At this point, the random generators created still maintain the Zerocoin relation and there are no modifications in this section. The mint parameter follows where outputs from the Setup mechanism are used to create a zero-knowledge proof which helps verify ownership of a Zerocoin on the network. Now comes the spend parameter which takes the output of the mint to create a witness for the supposed solution. On the NIX network, the output from the spend is then sent to a one-time address on the network which is only communicated with the prover of the zero-knowledge proof. On the NIX chain, , a spent Zerocoin outputs to a NIX that is sent to an address that can only be accessed and viewed by the receiver and payee. Since the payee is the Zerocoin accumulator in this instance, privacy is key between the receiver only.

This process works as follows: the transaction is created and is sent to N', where N' is the equivalent to a NIX public key paring hashed with a one-time address. In this case, N' is displayed as a NIX one-time address on chain that has no link to real NIX addresses. Because of this, Zerocoin can essentially be created and spent right away via a one-time address platform since monitoring these outputs can only be decoded between the receiver/user. This does not affect the Verification parameter for our trustless Zerocoin setup as the signature of knowledge is not affected by this method. Peers are still able to verify the signature of knowledge with the known public parameters.

Now poses the issue of monitoring peers which commit Zerocoin transaction to the mempool. Because there is a possible way for an attacker to monitor a user's interaction and transaction process via the networking in the P2P network, Tor networking allows obfuscation with no exit nodes which provides a networking trustless setup to prevent against these attacks, TOR is enabled by default in the NIX platform setup.

1. Ghost Protocol Overview

The NIX Ghost Protocol will consist initially of several privacy elements that will be continued to be built on top of. At launch, the NIX platform will enable Zerocoin with one-time-addressing outputs, i.e., stealth outputs coupled with Tor networking. Zerocoin helps scramble user data by creating a system that makes it impossible to guess the correct original location of assets. The stealth outputs create a blockchain element that conceals the destination output resulting in a non-traceable address location. These two mechanisms provide receiver and sender privacy. Integrated with a layering of Tor networking, users will have both blockchain privacy as well as networking privacy. The use of Bulletproof integrations will keep being researched and developed into the NIX Ghost Protocol, yet will not be available on main-net release.

2. Zerocoin Protocol

To solve the dilemma of anonymous transactions, Bitcoin and preceding alternative cryptocurrencies have attempted to use transaction mixers or ring signatures. However, there are a number of drawbacks to these proposed solutions. For one, a malicious or compromised member of a mixer or ring signature can break privacy. Furthermore, the anonymity set is a key metric to understanding how private a currency is. Privacy in formerly proposed solutions is limited by the size of the mixing cycle or ring signature. Each mixing cycle or ring signature is controlled by the number of transactions per cycle, which is transitively limited by the block size of the currency. Thus, the anonymity set in previous attempts at privacy tends to only be a few hundred transactions.

The Zerocoin Protocol is a strong encryption system in which large prime numbers are multiplied and the factorization of the resulting number makes it impossible to find out

which numbers were used[1].

With Zerocoin, the anonymity set is on a dramatically higher magnitude. Instead of having it limited to the few dozens, NIX, with the use of Zerocoin has an anonymity set that encompasses all minted coins in a particular RSA accumulator that can scale to many thousands, and -unlike other solutions- it is not subject to transaction graph analysis.

3. Bulletproofs Integration[2]

In general, privacy for payments are separated into two properties: (1) anonymity, hiding the identities of sender and receiver in a transaction and (2) confidentiality, hiding the amount transferred. While some digital currencies provide some weak anonymity, most of them lack any confidentiality. This is a serious limitation and could be prohibitive for many use cases.

Bulletproofs is a new ZK proof integration of creating confidentiality, as so, they do not require a trusted setup. The outlying solution which Bulletproofs bring is designing a trustless setup that creates transaction output privacy for users. Along with the integration of the Zerocoin Protocol, a user will now have access to not only location privacy of their coins, but also value privacy.

Bulletproofs is based on the notion of confidential transactions introduced by Maxwell in order to address the confidentiality of the amounts; the input and output amounts in a transaction are hidden in Pedersen commitments, meaning that every trade quantity involved is hidden from public view using a commitment to the amount. To enable public validation, the transaction contains a zero-knowledge proof that the sum of the committed inputs is greater than the sum of the committed outputs, and that all the outputs are po-

sitive, namely they lie in the interval [0,2n], where 2n is much smaller than the group size.

Whilst Bulletproofs have many applications, they are crucial for NIX to provide users with totally private transactions, aiming to achieve a truly distributed and secure environment to trade digital currencies.

4. Zerocoin Stealth Outputs

Zerocoin stealth outputs provide a way of concealing the destination address on chain by creating a hashing mechanism between the sender and receiver on the blockchain. This covers the actual NIX address that will be receiving the data on the network and reflects a stealth output to the public chain. Because the sender for the Zerocoin information is not one entity, the only compromise of data regarding the security of the stealth address is the receiver – i.e., the user. This ensures complete privacy of receiving Zerocoin payments.

5. Tor Anonymity Network

Tor is a software that enables the ability to conceal user location and usage from outside monitoring entities. When using Tor, a user's networking is routed through thousands of different network relays to scramble initial internet traffic resulting in a secure system for networking. Tor will be a default networking tool enabled in the NIX Platform.

[1] Zerocoin: Anonymous Distributed E-Cash from Bitcoin. Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin. The Johns Hopkins University Department of Computer Science, Baltimore, USA.

[2] Bulletproofs: Short Proofs for Confidential Transactions and More. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Stanford University. University College London.

1. NIX Core Beliefs

To create a powerful and decentralized system such that as the one NIX aims to enable, there are multiple elements which hold core to the value and dedication of the project. To reflect on the partnership with Blocknet, the team at NIX believes that Blocknet shares the vision of a truly decentralized environment to help empower people all around the globe. Up until now, some members of NIX team have focused and dedicated their time on Zoin, a community driven open sourced currency; they believe that the Zoin network of individuals are the essence of how there can be an immunity towards community driven empowering ecosystems. With that, as they carry their focus onto NIX, they wish to pay homage to the community and users of Zoin by issuing the initial circulation creation solely based from Zoin, with no ICO.

2. Initial Airdrop Supply

The team believes that in order to realize the unique and powerful NIX ecosystem, a new coin/chain must be created and molded with new specifications, rather than continuing to build on top of Zoin. However, because of their relationship with the Zoin community up until now, Zoin will be the only coin that will be given the opportunity to participate in the NIX Airdrop. There will be a 2:1 ratio of NIX to Zoin coins. In short, the NIX supply will be created with 2 times as many coins that Zoin will have in circulation at the time of a snapshot. Then a claimed airdrop will be initiated instead of an automatic one, having as evident benefits: a.) Rewards for Zoin shareholders - the initial coin circulation of NIX will come only from the NIX-Zoin Airdrop, and b.) The fact that not all coins may be claimed. Remaining unclaimed coins will be allocated towards a fund for research and development for the NIX protocol.

3. Specifications and Economic Model

NIX's specification set is created with one parameter in mind: the NIX/Zoin ratio based on circulation. This solution is outlined below. There will be a 7% network block fee that is allocated towards a development fund to continue the research and development of the NIX protocol. These developments will not only be directed at protocol enhancements and research, but also user and end-to-end interaction and usability. Currently there are 17.7 million Zoin circulating which creates NIX's initial circulation will be 38 million NIX with a 2:1 ratio and a 7% added coin creation to upkeep the 7% development fund.

Based on NIX-Zoin Airdrop

i.	Block Time	120 seconds (2 minutes)
ii.	Block Reward Halving	1,050,000 Blocks
iii.	Initial Reward	64 NIX
iv.	NIX Ghost Node Percentage	28%
v.	Miner Percentage	65%
vi.	Development Percentage	7%
vii.	Initial Circulation	38,000,000 NIX
viii.	Max Circulation	175,000,000 NIX
ix.	Zoin Swap Ratio	2:1
x.	Bitcoin Core Version	0.16
xi.	Algorithm	Lyra2REV2
xii.	Governance	Full Network
xiii.	Privacy	NIX Ghost Protocol

NIXPLATFORM.IO

NIX Platform whitepaper v1.0