NIX PLATFORM

Whitepaper 2.0

November 14, 2018

Table of Contents

I. Introduction and Concept

II. Protocol Layer

III. Utilization Layer

IV. Communication Layer

V. dApps Layer

VI. Conclusion

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.

Aside of common known centralization problems, lack of privacy adds a second issue, not only to traditional financial systems, but to cryptocurrency transactions as well. Financial privacy has become a rare and valued commodity; purchases performed via credit cards and bank transfers are monitored. It is possible to determine a lot about one person by analyzing spending habits. Sensitive financial information is currently being stored in systems that are highly vulnerable to being compromised.

As Bitcoin came to solve some centralization problems by providing the liberty of transacting with others without third parties involved, it has not, however, been able to provide complete financial privacy as transactions can still be linked to individuals.

2. Objectives and Purpose

NIX aims to grant the means and resources to 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 is adopting 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 offers layered optional privacy that is enabling people to create a medium of communication and dApps between blockchain channels, for whichever purposes each channel stores.

3. Intra And Interoperable Privacy Platform

NIX is being built to establish an ecosystem of asset distribution with the added power of privacy. To achieve this, the initial design targets a series of strong intra-chain privacy elements, like the **NIX Ghost Vault** and **2-Way Ghosting**, to first make NIX a powerful privacy based coin.

To deliver the above mentioned features, NIX has created a personal privacy library named the **NIX Ghost Protocol**, which is using the mechanisms of Zerocoin privacy proofs, paired with one-time integrated Zerocoin addresses. This is also combined with a Tor network that offers OBFS4 bridging and communication. All elements from networking privacy to blockchain privacy are offered.

Along with the **Ghost Protocol**, an atomic swaps infrastructure is being developed to allow private transactions among different chains. This layer focuses on chain-to-chain private transfers via NIX Platform.

4. Privacy Features Overview

The **NIX Ghost Protocol** consists of several privacy elements that will be continued to be built on top of. NIX platform has enabled Zerocoin 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. Integrated with a layering of Tor networking, users 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 is not available on mainnet release.

Based on the **Ghost Protocol**, NIX developed its first privacy solution, **NIX Ghost Vault**. This feature provides full one way privacy to either the sender or the receiver and allows users to completely hide coins from the chain.

Apart from NIX Ghost Vault functional feature, NIX has crafted the first in history privacy-in-one-transaction development: **NIX 2-Way Ghosting**. This innovative development allows users to transfer their private coins from one vault to someone else's vault. To enable 2-Way-Ghosting, NIX designed and implemented Commitment Key Packs. **Commitment Key Packs** allow for an address-less blockchain payment protocol which has never been done before utilizing Zerocoin.

These privacy features are explained with details in the present document.

5. NIX Multi-Layered Scheme

NIX is a multi-layered privacy currency which utilizes an interoperable platform model to fuel privacy focused decentralized applications. By definition it covers 4 main layers: **Protocol Layer**, containing the consensus mechanisms and privacy protocol design; **Utilization Layer**, which includes tools and features like the Ghost Vault and 2-Way Ghosting; the **Communication Layer**, accounting for interoperability between chains; and the **dApp Layer** which extends to dApp development and use cases such as the DEX Manager.

II. Protocol Layer

1. Proof-of-Stake consensus

The objective of a cryptocurrency security system is to ensure that remote processes arrive at the same conclusion in perfect order, this is known as consensus among nodes. All nodes in the network must record every single transaction, which is achieved by the consensus protocol.

NIX Platform employs Proof-of-Stake consensus mechanism to secure the network, validate the blockchain and allow the emission of new blocks. NIX holders (stakers) act as nodes that account for the execution of those tasks; as a result, their voting power on the network validation process is proportional to the amount of NIX coins they stake and thus their staking reward frequency.

Proof-of-Stake technology complements NIX's core value of decentralization, as mining monopolies that manipulate blocks become abolished and it does not involve the creation of new units of money.

2. 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.

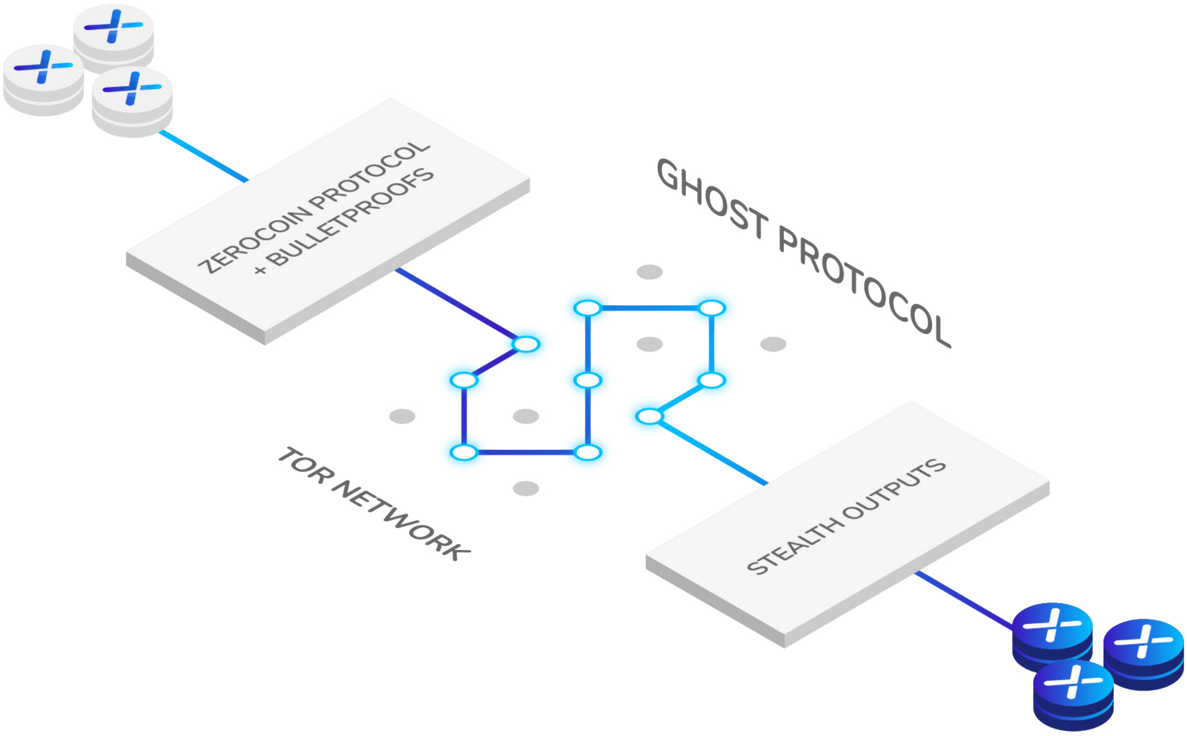
With zero-knowledge proof elements for concealing transaction and data movements along with the Zerocoin Protocol and Commitment Key Packs scheme, the NIX privacy protocol is the most robust and mathematically secured cryptocurrency system.

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.

Initially, a setup parameter is designed in order to create an accumulator environment with prime numbers p and q such that $p = 2^{\omega}q + 1$ for $\omega \geq 1$. 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/user 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. Proof-of-Stake consensus



2.1. Zero-Knowledge Proofs

Zero-knowledge proofs are proofs that show a statement to be true without revealing anything other than the veracity of the statement to be proven[1]. They are particularly effective in fields like secure communication, privacy and authentication.

By definition, a zero-knowledge proof must satisfy the following three properties: Completeness, the high-probabilistic opportunity that if the part A is telling the truth, the part B is being convinced that part A is telling the truth. Soundness, the fact that part A can only convince the part B if it is telling the truth. Zero-knowledgeness, the fact that the part B does not learn anything about the part A's knowledge.

NIX Platform uses zero-knowledge proofs to help anonymize transactions; in detail, they allow NIX to obfuscate information of transactions on the public blockchain network.

2.2. 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 are used[2].

With Zerocoin, the anonymity set is on a dramatically higher magnitude. Instead of having it limited to the few dozens, the NIX network, 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.

2.3. Pedersen Anonymous Deposits: Commitment Key Packs

The introduction of zero-knowledge commitment schemes using Zerocoin Protocol techniques allows for anonymous coin mixing on a blockchain which enables coin history destruction and full parameter privacy. Currently, Zerocoin is enabled as an intra-layered protocol for individual clients on a P2P blockchain network. The NIX network proposes a solution that expands the isolated zero-knowledge scheme towards a commitment key pack solution that allows third-parties to conduct in direct zero-knowledge payments resulting in an address-less blockchain payment protocol.

As a soft-fork implementation, a new key scheme can be created which manages and tracks Zerocoin Pedersen commitment values for direct public deposits. To understand how this does not compromise any parameter information from peer to peer, NIX breaks down the Zerocoin payment layout as follows:

To create a Zerocoin Mint, several private parameters are used in order to generate the single public parameter that is shared to the network. A random private ECDSA key is created with every single Zerocoin Mint object, in turn a pairing public key (P) is generated. The public key is then RIPEMD160 hashed into a serialized object to create (S). Finally, NIX Platform then generates a large random number (R) that is used to compute the Pedersen Commitment (C) for the Zerocoin through use of RSA-2048 as the modulus commitment group. The one public parameter that is now serialized and transmitted through the network is the Pedersen Commitment (C).

NIX created a key scheme called Commitment Key Packs that allows packing of Pedersen Commitments to act as one-time-key formats for Zerocoin Deposits. Through this, NIX can conduct full blockchain privacy payments without the need of using any group-able addresses on chain and instead conduct transactions using only zero-knowledge commitment schemes. A Commitment Key Pack creates a simpler environment for clients to manage one-time payment locations. By default, Zerocoin works as a fixed denomination payment model, and because of this, each individual Commitment Key can only accept one deposit. The purpose for a Commitment Key Pack is to allow a key format to group commit schemes to permit peers to conduct multiple zerocoin transactions at once.

Flexibility: This privacy model requires a partial interactive payment setup between peers. Because keys are one-time usable, providing the same key to multiple payees is not accepted, therefore a custom Commitment Key Pack should be provided to each payee. Verification of the payment can be monitored in an offline manner, yet ownership of the payment cannot be verified offline.

Scalability: A drawback to this current model include lengthy and unfriendly key formats. Because this payment protocol requires a partial interactive payment setup, the encumbrances of lengthy keys do not pose a major issue, yet this could be mitigated in the future by enabling sender-receiver parameter calculations. This could be done by compromising one of the private parameters such as the random number (R) used to calculate the Pedersen commitment (C) to be calculated instead by the sender. In this case, the receiver only needs to provide a Commitment Key Pack which packages the public key hashed values which are much smaller in length. Another design that could be used to lessen the key length is integration of bulletproofs to introduce reduction of proof sizes which will directly affect the Pedersen commitment size in turn the Commitment Key Pack. Both these solutions are being looked into further.

Design: To allow for flexibility in the key scheme, the design of a Commitment Key Pack reflects the following encoding format.

Base61(C0 + ... Ci + 0xFFFF(eokp) + CSize0(1byte) + ... CSizei + checksum(4bytes))

A 4 byte eokp (end-of-key-pack) identifier is placed at the end of the grouped commitment keys, followed by respective sizes in single byte increments followed by a 4-byte checksum. This allows keys to be created based on any amount of Commitment packings which allows for flexibility in one-time payments, however big they may be. A 10-packed amount is enabled by default, nonetheless simple parameter changes can modify it in the base client.

Implementation: Because Commitment Key Packs do not work like standard key pairs, it is necessary to continually scan each block for a direct match. However, no strenuous calculations are made to determine whether or not a payment has been successfully transferred, so the check can be made in O(1) time which in turn adds negligible time to the blockchain sync process.

When a localized Zerocoin is created currently, the Zerocoin data is written to the wallet database which is then used to provide the ZK proof on Zerocoin spend verification. However, Commitment Key Packs differ in that the ZK proof information is instead stored on a separate wallet database that is used to either generate packs for payments, or to scan each block or transaction to verify ownership.

With Commitment Key Packs being an interactive payment model, simple SPV wallets can be dedicated to hosting the one-time-keys associated with these payments. To determine if an existent paid Commitment Key Pack is eligible to redeem on the blockchain, only two factors must be known, the public commitment scheme, and the serialized private coin information. With these two parameters, a light wallet does not need to sync with the entire blockchain, and instead, only needs to create a data structure that holds total public and private redeemed commitment schemes on chain. This can be an extremely light performance based process, and broadcasting payments to the network does not require pre-existing blockchain history.

Benefits: There are many factors that could potentially break a user's privacy on a single blockchain. Commitment Key Packs create an environment of privacy that cannot be broken by any external parameter. One privacy failure could be IP linking through node transaction transmission, which can help group and identify transactions made by certain nodes to one owner. A work-around for this would be to use Tor/VPN and/or Dandelion. The issue here though comes when a transaction is funded from multiple change addresses, linking the owner and previous blockchain history rendering the Tor/VPN and/or Dandelion useless. To be almost 100% private on all ends of a transaction, a user would always need to make sure proper networking and blockchain privacy is managed; this could add inconveniences to the process of transacting on a specific blockchain network. With Commitment Key Packs, there is no need for any networking privacy since transactions cannot be linked to public any UTXO sets. Theoretically, if a user only conducts transactions using Commitment Key Packs, there could be no way of compromising his/her history.

Conclusion: NIX Platform has proposed a full parameter private address-less blockchain payment protocol which can be integrated through a simple soft-fork. The benefits that this payment model can offer, outweigh any encumbrances in its current state. This protocol not only enhances user privacy on a single blockchain, it also simplifies any layer-2 solutions utilizing privacy mechanisms.

2.4. Bulletproofs Integration[3]

Bulletproofs is a zero-knowledge proof integration of creating confidentiality. The outlying solution which Bulletproofs bring is designing a trustless setup that creates transaction output privacy for users whilst highly reducing transaction size.

This protocol runs on very short proofs and without a trusted setup; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values. This technology brings a significant improvement to the cryptocurrency ecosystem regarding proof size.

Bulletproofs is based on the notion of confidential transactions introduced by Maxwell in order to address the confidentiality of the amounts. 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 positive, namely they lie in the interval [0,2n], where 2n is much smaller than the group size.

As a consequence, Bulletproofs increase in size only logarithmically with the number of outputs and size of the range's proof, as a result, the size of transactions get reduced significantly. This implementation can turn into huge space savings, faster transactions and incredible space savings.

Bulletproofs technology application is being studied to be incorporated to the NIX Network as a scaling solution.

2.5. 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 is a default networking tool enabled in the NIX Network.

2.6. Dandelion

The integration of Dandelion to the NIX Network provides an additional level of privacy by way of concealing the IP address of a user broadcasting a transaction.

When a user (A) wishes to transfer funds to another user (B), A generates a transaction message that includes some of his/her information: the quantity of funds transferred, the prior transaction from which these funds are drawn, and a reference to B's pseudonym. The system-wide sequence of transactions is shared and broadcasted to the nodes that the network is connected to and recorded on a public blockchain in a very fast manner[4].

Considering the current node's communication protocol and given the wide propagation range of user's information to many nodes, it can be inferred that, if several conditions are reached, the IP address that conducted the transaction could be discovered, thus compromising user's privacy.

Dandelion modifies the communication protocol among nodes by implementing 2 processes called: stem phase and fluff phase. The stem phase changes the traditional model of broadcasting a transaction to all nodes at once, instead it gets communicated from node to node. Each time a node receives a stem-phase transaction from another node, it either relays the transaction or diffuses it, which brings the second phase.

Once this information has been shared from node to node, the fluff phase reconfigures the communication mode back to traditional system, i.e., all connected nodes are informed about the transaction. As the nodes that originally shared the information in the stem phase do not do it in a public way, it highly decreases the probability of finding the user who conducted the transaction.

3. NIX Ghostnodes

NIX Ghostnodes help to ensure dedicated network processing for Ghost Protocol transactions. Any smart contract based element that requires autonomous privacy processing relies on the NIX Ghostnodes to fulfill that request. Maintaining and running a NIX Ghostnode is a decentralized process in which users need to obtain 40,000 NIX coins to run. By holding these NIX coins in 'G' addresses and following Ghostnode setup procedures, the network uses nodes to dedicate power for NIX Ghost Protocol transactions ensuring no bottleneck in the computing component of each privacy element; in return, each Ghostnode is rewarded as follows: a.) There is a 0.25% fee awarded to NIX Ghostnodes through any Ghost Protocol transaction 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 Ghostnodes additionally earn partial block rewards of around 70% per block.NIX Ghostnodes

1 - A Survey of Zero-Knowledge Proofs with Applications to Cryptography. Austin Mohr. Southern Illinois University at Carbondale, USA.

2 - 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.

3 - 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.

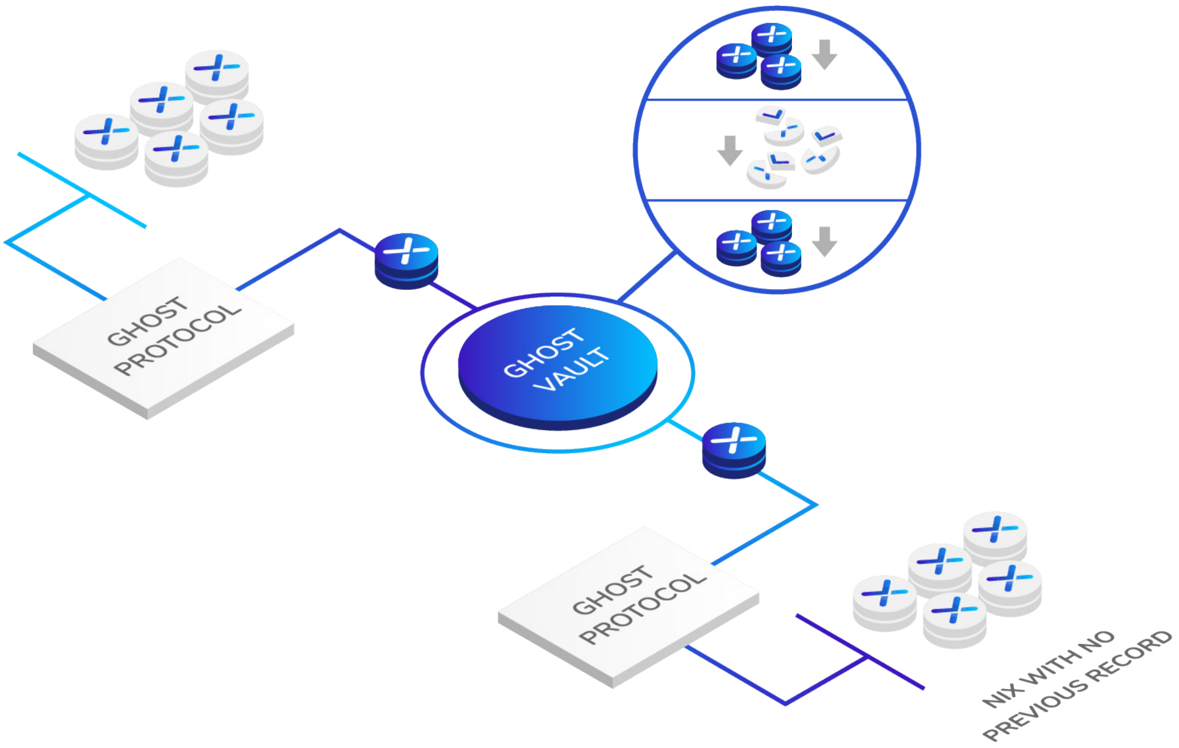
4 - Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller and Pramod Viswanath.

1. NIX Ghost Vault

NIX Ghost Vault is a privacy feature based on the Ghost Protocol that makes user's coins completely private from the chain. This element uses Zerocoin to conceal transaction location with one way privacy: either for the sender or the receiver.

This is the first Ghost Protocol privacy solution as it allows users to mint NIX coins, essentially making them disappear with no previous history and permitting the user to decide when to spend their coins leaving no traces for NIX.

Ghost Vault functioning is similar to a Zerocoin accumulator which privatizes location Zerocoin Mixing. NIX are not directly stored in the Vault, as they are first minted into zerocoins by the implementation of the optional privacy Ghost Protocol. As this system works similar to an accumulator by combining everyone's minted zerocoins, what is of public knowledge is the number of zerocoins there are on it, therefore there is no way to identify which coins belong to each user, which in turn results in complete anonymity. The overlying feature of the Ghost Vault is the more users and volume going in, the greater the privacy set for everyone utilizing the Ghost Protocol.



With this feature, each user is able to send coins to their Ghost Vault which then hides the locations of those coins. Sending coins to the Ghost Vault is called "ghosting", this process is fully private for receiver, as the destination is a hidden location, yet the sending address is public and identifiable. Sending coins from the Ghost Vault is called "unghosting", here the sending address, represented by the vault is private, giving sender privacy, yet the receiving address is public.

As the Ghost Vault uses the Ghost Protocol, it generates fees to Ghostnodes when users conduct public to private payments, so 0.25% of the coins stored into the vault is distributed among nodes as a form of income for backing the private transaction. Commitment Key Packs scheme transactions (Zerocoin to Zerocoin payments) are feeless.

1.1. Ghosting and Unghosting

Zero-knowledge proofs are created whenever a public NIX coin is ghosted which is then serialized into a format for specific transaction inputs and outputs. The specific format for these deployments are as such:

For a NIX coin being ghosted, the NIX Network utilizes the OP_ZEROCOINMINT opcode which enables peers to read and store the transaction script as a zerocoin into the networks accumulator:

Vin:
Public NIX coins

```
Vout:
CScript() <<
OP_ZEROCOINMINT <<
pubCoinValueSize <<
pubCoinValue;
```

This is a simple storage of the Zerocoin model that was created when NIX coins were being destroyed and ghosted. With this, the network communicates that there has been a NIX coin destroyed, and in turn a zerocoin has been made.

For a ghosted NIX coin to be unghosted from its zerocoin format, NIX Platform utilizes the OP_ZEROCOINSPEND opcode which enables peers to read and validate the zerocoin spend script as it attempts to convert a zerocoin into a NIX public coin. The specific format for these deployments are as such:

```
Vin:
CScript() <<
OP_ZEROCOINSPEND <<
serializedCoinSpendSize <<
serializedCoinSpendProof;
```

Vout:
Public NIX coins

Here, the zero-knowledge proof to the original Zerocoin is attached to the transaction for the network to validate. This entire process allows the destruction and recreation of NIX public coins in two steps.

2. NIX 2-Way Ghosting

To enable full transaction privacy between sender and receiver, NIX Platform introduced the 2-Way Ghosting mechanism, which is based on our **Commitment Key Packs** scheme.

2-Way Ghosting adds the ability to mint new zerocoins when unghosting and deposit them into receiver's Ghost Vault.

This brought NIX Platform towards enabling the faculty to launch powerful private smart contracts on chain while allowing end-to-end Zerocoin private transactions, a never-done before implementation.

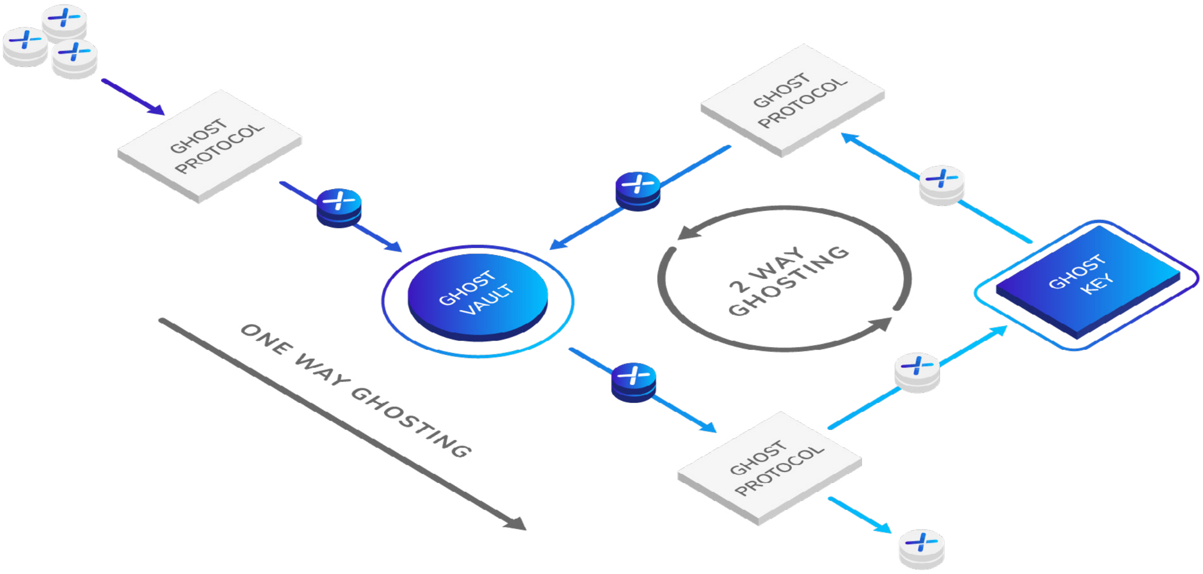
2.1. Application

For being ghosted, NIX coins go through the Ghost Protocol which destroys NIX and converts them into zerocoins. The vault represents a cryptographically secured place where those zerocoins are stored and become impossible to trade from the chain as they get mixed with other user's zerocoins.

Once in the vault, coins can be transferred to two different locations. The original format is then sent to a public NIX address. Meaning zerocoins are unghosted and thus converted into new NIX. As the receiver is a public NIX address, those NIX can be traced throughout the blockchain, therefore they are no longer private.

To eliminate one way privacy issues, NIX employs a Key List containing customized one-time-keys (Ghost Keys) based on the Commitment Key Packs scheme; they can be found in NIX core wallet and are used to unlock zerocoins.

The receiver must provide the sender with one Ghost Key, and now, instead of ghosted NIX being sent to one public address, they are converted into new ghosted NIX, sent to a Ghost Key and progressively to the receiver's Ghost Vault. As it can be noticed the whole process is performed without involving public addresses and without compromising user's security as once a Ghost Key gets used it gets burnt.



3. NIX Ghost Vault Staking

NIX Platform is planning the incorporation of Ghost Vault staking so that users keeping their coins private in the vault do not miss rewards.

This feature, aside of keeping coins private, is capable of increasing NIX Platform privacy set as it incentivizes users to stake their coins in the form of Zerocoins directly from the Ghost Vault.

IV. Communication Layer

The purpose of this layer is to incorporate different platforms, allowing them to build on the NIX Network to access various blockchains in a privacy agnostic fashion. The cross-chain atomic swaps infrastructure that is being built on NIX plays an important role in this ecosystem, not to mention that privacy is the key factor to be provided within this interoperability infrastructure.

1. Inter-Communication Model

The creation of an inter-communication model within the NIX environment points multiple elements. The utilization of privacy centered smart contracts allows for dApps to fill the space for inter-chain communication protocols.

Branching outwards, the NIX architecture proposes the creation of any chain-to-chain communication layer to use the privacy metrics that NIX offers. Not only NIX provides value in its own financial ecosystem, it also consents utility in a smart contract privacy system. NIX aims to 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 creating on the platform entitle users to deposit NIX into a network distributed address, this address fulfills agreement requirements in the establishment of the communication model.

2. 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 permits network customization without requiring a change in the NIX core protocol. This plays a big role in NIX’s direction at solving supply chain management through blockchain.

V. dApps Layer

The dApp layer consists of decentralized applications running on top of the NIX Network utilizing NIX's unique privacy protocols. DApps economize digital resources providing a way to monetize what has previously been very difficult to do. The NIX dApp layer provides the option of full privacy for all of these digital assets utilizing NIX privacy protocols.

The first case of a dApp in the creation of NIX ecosystem is the bridge between DEX platforms in delivering a privacy layered system to privatize atomic swaps. The DEX Manager looks forward to solving privacy layers among DEX trading while also connecting all joined DEXes allowing for much greater amounts of liquidity.

1. 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 manager.

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. By integrating several DEX platforms, NIX Platform allows for the exchange of one cryptocurrency for another without the need of a trusted third party.

This system creates a layer of privacy for any protocol and tradeable asset through a multi-tiered trading structure. NIX seeks to bridge communication within external DEXes to create privacy elements among all and any compatible ecosystems. The progressive incorporation of more DEXes is allowing NIX to achieve this system unification, permitting direct development on each protocol in a streamlined fashion as a prompter integration is developed.

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. This is possible with any decentralized exchange protocol that gets integrated into the NIX Platform.

NIX Ghost Protocol transactions are conducted by means of the NIX Ghostnodes 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.

NIX Ghostnodes work to accomplish these consensus requirements. Any integrated DEX communication model is handled between NIX Ghostnodes on the NIX Network. With the NIX consensus system utilizing Proof-of-Stake on chain, NIX Ghostnodes are used to approve and fulfill cross chain protocols. The use of NIX Ghostnodes generates an automation of network privacy for these created ecosystems.

VI. Conclusion

1. NIX Core Beliefs

To create a powerful and decentralized system such as the one NIX aims to enable, there are multiple elements which hold core to the value and dedication of the project. The NIX Network believes that it is mandatory to focus on the vision of a truly decentralized environment to help empower people all around the globe while combining not only technical resources but also strong forces that work to finally provide cryptocurrencies with what they need: privacy and decentralization.

2. Specifications

The following represents NIX's specifications: Specifications

I. Block Time	120 seconds (2 minutes)
II. Block Reward Halving	Every 4 years for Ghostnodes
III. NIX emission by staking	1.5% of circulating supply
IV. Total Block Reward (starting at 40 million NIX circulating supply)	~12.01 NIX
V. Initial Circulation	38,000,000 NIX
VI. Bitcoin Core Version	0.17
VII. Block emission	Proof-of-Stake
VIII. Governance	Full Network
IX. Privacy	NIX Ghost Protocol

3. NIX Network Future

NIX's final goals are to provide full privacy and decentralization, so we are moving forward towards those goals by delivering privacy-based solutions that are the foundation of NIX Platform's use case and by moving to a more decentralized ecosystem, one in which any developer can build on top of.

The NIX Network forsees the future as follows: Having **Utilization Layer** applications being widely and promptly implemented as well as accomplishing private trades between chains, which encompasses NIX's **Communication Layer** goals.

Subsequently, the network looks forward to the launch of NIX's DEX Manager as the first **dApp Layer** solution. This is intended to become a user friendly application that, as a privacy tool, executes transactions among different DEXes.

Ultimately, NIX's purpose is to become a completely decentralized project, where no main teams nor development funding are needed, instead, having several teams that work on different areas to update the core code whilst offering tool kits for other developers to create their own dApps using NIX's privacy utilities.

NIX

NIXPLATFORM.IO

Nix Platform Whitepaper 2.0