

Mixin Network

A free and lightning fast peer-to-peer transactional network for digital assets.

CRYP2NOVA

TECHNICAL WHITE PAPER SUBJECT TO FURTHER REVIEW AND UPDATE

Archived copy · cryp2nova.com

Contents

1. Motivation
2. Overview
3. Mixin Kernel
    3.1. Ghost Output
    3.2. Asynchronous BFT Graph
    3.3. Punitive PoS
    3.4. Trusted Execution Environment
    3.5. Light Witness
4. Mixin Domain
    4.1. Kernel System Calls
    4.2. Standard Domain Interfaces
    4.3. Domain Extensions
5. Attack Resistance
6. Governance
7. XIN - The Token
8. Conclusion

CRYP2NOVA

Archived copy · cryp2nova.com

Motivation

Bitcoin started a new era for financial resources management. People have regained the power to manage their assets by themselves, to monitor how the resources are being distributed, and to rescue the economy from the control of the few.

Today, both professionals and the general public have accepted the idea behind Bitcoin and blockchain technology, and the user base of crypto currency is growing at a faster and faster pace.

Unfortunately, Bitcoin suffers from this fast growing adoption. The most significant problems are insufficient transaction capacity, slow confirmation and high transaction fees.

Due to the inflexible highly distributed nature of Bitcoin network, it's impossible to fix some critical flaws. Rather than fix the original Bitcoin project, most people attempt to invent new projects that address different perceived shortcomings of Bitcoin.

Thus Ethereum, Monero, Stellar, Cardano and many new blockchains have been invented in the past few years. Almost all of them attempt to fix the problems of Bitcoin while adding some new features of their own. However, they are unable to rescue or augment the

Archived copy · cryp2nova.com

original Bitcoin network, and are neither able to interoperate with each other.

Fortunately, some Bitcoin believers are working on addressing Bitcoin's shortcomings, and they have proposed several excellent solutions. The most significant one is Lighting Network[0], which is a micropayment system built on Bitcoin network without requiring any modifications to Bitcoin code.

0. Lighting Network https://lightning.network

Another interesting solution is the Liquid[1] project from Blockstream, which is a federated and two-way pegged sidechain alongside Bitcoin blockchain.

1. Blockstream Liquid https://blockstream.com/liquid

All these attempts have put forward the entire Bitcoin network without sacrificing the security and distributed nature of the original Bitcoin vision. Similar solutions have been put forward on Bitcoin competitors, e.g. the Raiden Network[2] on Ethereum.

2. Raiden Network https://raiden.network

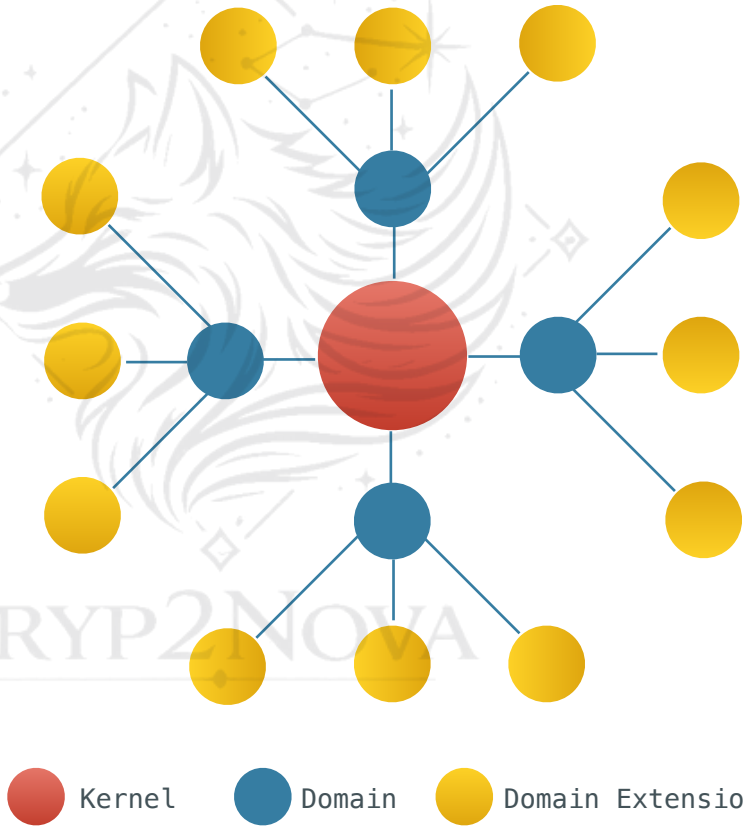
In this paper, we try to propose a solution that can empower all the popular distributed ledgers. We call this solution Mixin. Mixin is not about creating yet another crypto currency or a competitor to any distributed ledgers.

Similar to what Lighting Network and Liquid are for the Bitcoin blockchain, Mixin is a public distributed ledger to allow any public distributed ledgers to gain *trillions of TPS, sub second final confirmation, zero transaction fee, enhanced privacy and unlimited extensibility*.

Archived copy · cryp2nova.com

Overview

Mixin is composed of a single theoretically permanent Kernel, many dynamic Domains and different multi-purpose Domain Extensions, to formulate an extended star topology.



This topology may lead to the concern that Mixin is a centrally controlled network, but that's not the case because of how the Kernel itself works.

Archived copy · cryp2nova.com

Mixin Kernel is a high performance distributed ledger and its sole responsibility is to verify asset transactions. That said, the single permanent Mixin Kernel is also a distributed network just like Bitcoin network as a whole.

Although Mixin Kernel verifies asset transactions, it doesn't produce any assets. All assets flow through the Kernel by Mixin Domains.

Each Mixin Domain is also a distributed ledger, whose job is providing assets to the Mixin Kernel. The assets may be those on Bitcoin, Ethereum or any other blockchains, or even central organizations like banks.

While each Mixin Domain is a component to provide assets for Mixin Kernel, the Kernel itself is also a component in the Mixin Domain to verify and govern its assets.

Unlike most existing gateway based solutions, Mixin Kernel and Domains are all public available distributed ledgers, with no central authorities.

From the Kernel to Domains, the Mixin Network is all about assets and transactions. The Mixin Domain Extension is where the magic happens, whether for Ethereum contracts, EOS contracts, a distributed exchange on somewhat trusted instances, or anything else.

Archived copy · cryp2nova.com

Mixin Kernel

The core of Mixin Network is the Mixin Kernel, a fast asynchronous Byzantine fault tolerant directed acyclic graph to handle unspent transaction outputs within limited Kernel Nodes.

Ghost Output

Mixin Kernel utilizes the UTXO model of Bitcoin to handle transactions, and CryptoNote[0] one time key derivation algorithm to improve privacy, since there is no address reuse issue. We call the one time key a Ghost Address and the output associated with it a Ghost Output.

0. CryptoNote https://cryptonote.org/whitepaper.pdf

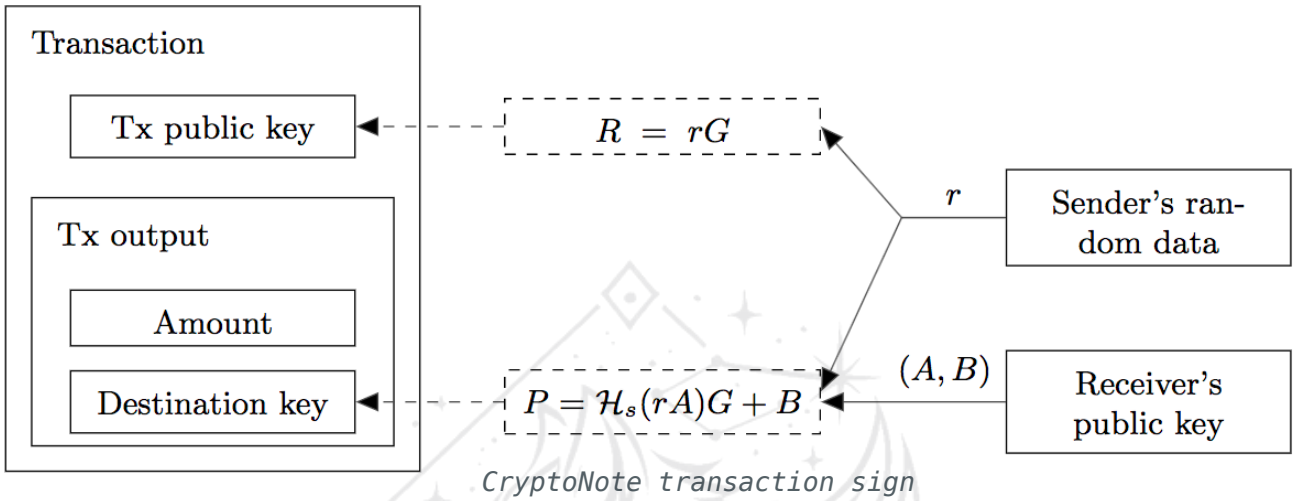
In the algorithm, each private user key is a pair (*a, b*) of two different elliptic curve keys, and the public user key is the pair (*A, B*) of two public elliptic curve keys derived from (*a, b*).

When Alice wants to send a payment to Bob, she gets Bob's public user key (*A, B*) and derives at least three Ghost Addresses with some random data, which ensures at least three different Ghost Outputs will be created for Bob.

The three Ghost Outputs threshold delivers better privacy, and also forces the outputs random amounts.

Archived copy · cryp2nova.com

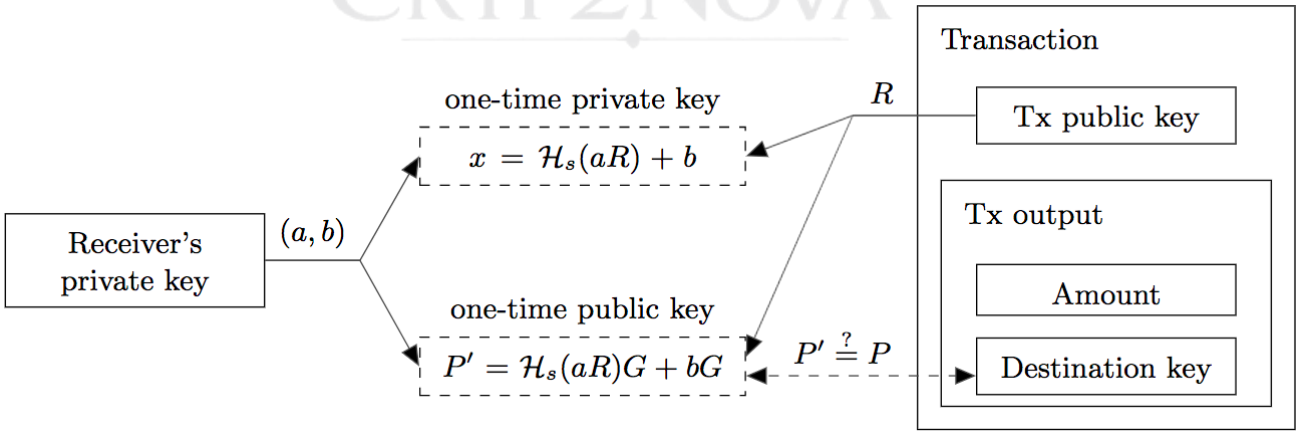
After deriving the Ghost Addresses, Alice will sign the transaction with CryptoNote algorithm.



CryptoNote transaction sign

Note that, to improve privacy, Alice is forced to pick random UTXOs as the transaction inputs. After the transaction is signed, Alice sends it to the Mixin Kernel.

Only Bob can recognize his transactions due to the Ghost Address feature, he can decrypt the output information with his tracing key (*a, B*).



CryptoNote transaction verify

Archived copy · cryp2nova.com

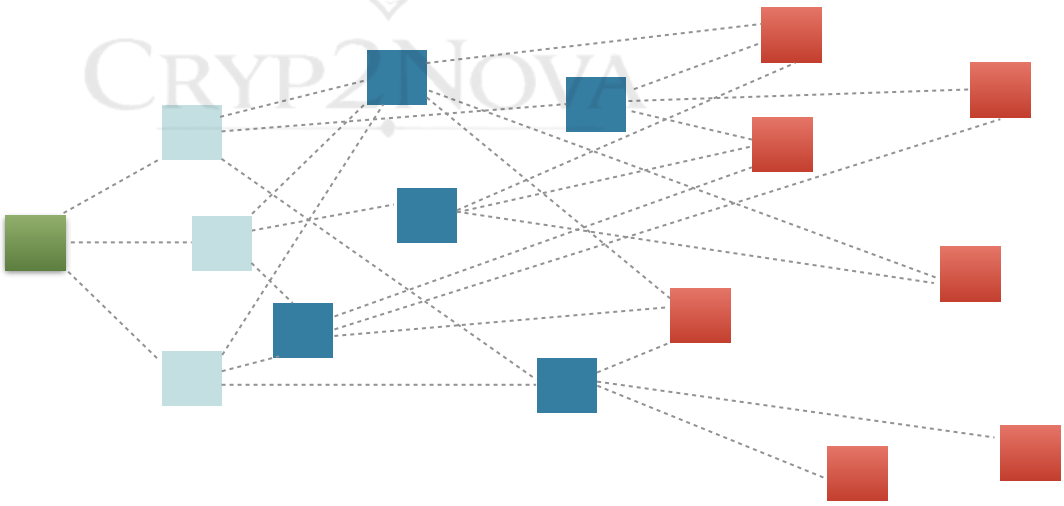
If an exchange wants to have a transparent address to disclose all its assets information publicly, it can just publish its tracing key (*a, B*) so that everybody can recognize all its transactions but can't spend them without the secret key *b*.

Asynchronous BFT Graph

0. Section XIN - The Token for details

Each Mixin Kernel Node is required to pledge 10,000 XIN, therefore due to the 500,000 XIN circulating supply[0], no more than 50 Kernel Nodes will exist. To prevent extremely centralized authority, the Kernel can only be booted with at least 7 Kernel Nodes.

The Kernel nodes make up a loose mesh topology, and are responsible for transaction validation and persistence. Unlike a blockchain, there are no blocks in the Mixin Kernel, all transactions will be exponentially broadcasted as soon as possible.



transaction flow when K = 20 and b = 3

Archived copy · cryp2nova.com

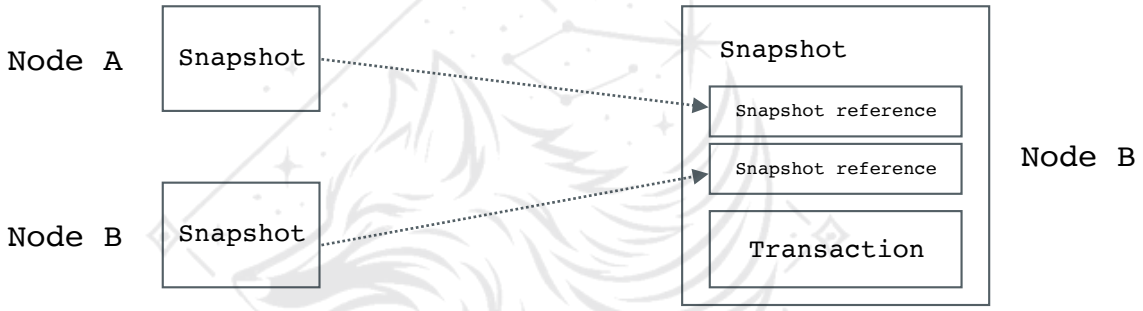
A typical Mixin Kernel transaction finalization sequence goes as follows:

1. When Alice's signed transaction is sent to the Mixin Kernel with *K* (*7 <= K < 50*) nodes, *b* (*b > 1*) random nodes (*A*) will receive it.
2. Each node does the same transaction validation.
    1) Inputs are all unspent.
    2) Input and output amounts are in valid range.
    3) Verify the signature of each input.
    4) The total of input amounts equal to the total of outputs.
3. Each node will create a Kernel Snapshot with the validated transaction, and the snapshot is the base unit stored in the Kernel to construct a DAG. Each snapshot is composed of:
    1) The transaction as payload.
    2) Previous snapshot hash of this node.
    3) The node signature.
4. The signed snapshot will be broadcasted to another *b* random nodes (*B*) as soon as possible. After received the snapshot and validated with the same procedure in step 2, a new snapshot will be created immediately. This snapshot has the same payload as received snapshot, and the referenced snapshot hash is a pair of previous snapshot hash in this node and the received snapshot hash.
5. Steps 4 will be repeated until the node learnt that wether the transaction is approved or rejected by at least *2/3K* nodes. Since each snapshot referenced the parents up until the nodes group *A*,

Archived copy · cryp2nova.com

it's easy for new nodes to learn that the previous snapshots are aware of the snapshots. This procedure can avoid lots of redundant works.

6. In this procedure, a transaction can be approved or rejected in about *K/b^2* rounds on average, considering the typical Kernel size, the latency may be within a single second with very high probability and guaranteed within seconds.



Due to the asynchronous BFT consensus, double spend is impossible. Because of the UTXO nature, snapshots order is irrelevant and high concurrency can be guaranteed in the DAG.

Punitive PoS

Each Mixin Kernel node takes 10,000 XIN, which is approximate 2% of the network stake. The Kernel can only operate with at least 7 nodes joined, or about 15% of the whole network stake.

The Kernel BFT consensus is secured by a strict punitive PoS, if a Kernel Node is determined to be an

Archived copy · cryp2nova.com

attacker, all its collateral will be recycled to the mining pool. The node will be identified as an attacker if it tried to broadcast an obvious double spend snapshot. A snapshot will be considered obvious when some of its inputs state have been validated by at least *2/3K* nodes.

The first time a node sends out an attacking snapshot, its stake won't be recycled, but it will be flagged by the network as a potential attacker. The Kernel size will be temporally reduced to *K - 1*, with this reduction invisible to the potential attacker.

All other nodes will still broadcast to the flagged node, but won't consider its snapshots in stake votes. If further snapshots from the flagged node remain malicious, the Kernel will sign a snapshot with a transaction that will transfer all the flagged node's collateral to the mining pool.

The flagged node will be permanently removed from the Kernel and it will have some period to appeal to Mixin Kernel Governance[0], which is voted by all XIN holders.

0. Section Governance for details

Trusted Execution Environment

Mixin Kernel is already an ABFT consensus DAG. To ensure further security, Kernel nodes must run in Trusted Execution Environment[1]. Specifically, Mixin uses Intel SGX[2] as the TEE implementation.

1. Trusted Execution Environment https://en.wikipedia.org/wiki/Trusted_execution_environment

2. Intel SGX https://software.intel.com/en-us/sgx-sdk/details

Archived copy · cryp2nova.com

The TEE enforcement ensures three important security and trust factors in Mixin Kernel.

1. All Kernel nodes should run the same consensus ruleset.
2. Mixin Kernel will be trusted due to the Intel SGX enclave, even when the Kernel is controlled by several earlier Kernel nodes.
3. Distributed Domain communications will be much more secure.[0]

0. Section Kernel System Calls for details

The underlying logic for the TEE security is that Intel SGX is somewhat trusted for the Mixin system.

Note that, Mixin Kernel is secure by itself, at least as secure as existing BFT solutions. The mandatory Intel SGX just makes it better.

Light Witness

Mixin Light node is a simplified payment verification (SPV) node to Mixin Kernel. It typically stores all its unspent outputs for easy account balance query.

If the Light node is a XIN holder, it has the chance to act as a Light Witness. The Light Witness will actively monitor the Mixin Kernel, and will be scheduled to vote automatically on the attacker appeals.

The Light Witness vote is weighted on their XIN stake. And the vote is mostly on the attacker node's network

Archived copy · cryp2nova.com

connectivity state to determine whether the attacker behavior is caused due to network delay.

All the Light Witness votes will be weight calculated with the Mixin Kernel Governance votes, to determine the final attacker appeal. If the appeal fails, the penalty will be final.

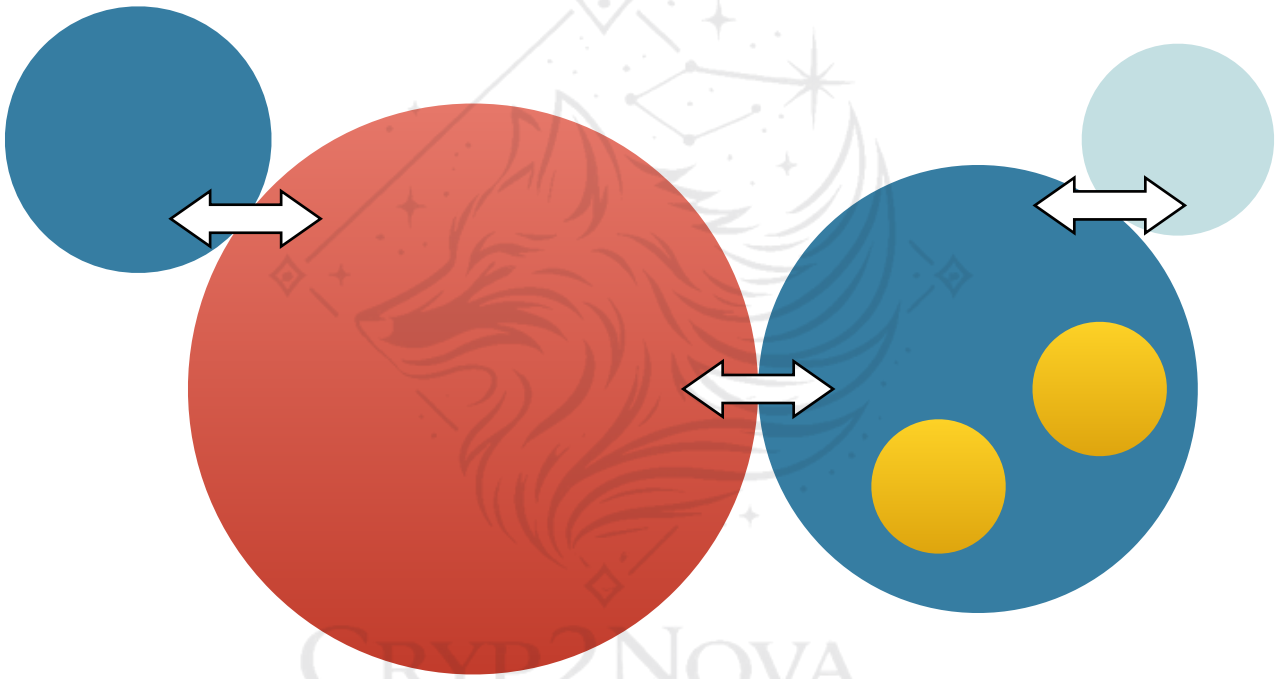
The Light Witness is incentivized to do these votes because they could get the mining reward if they do some work for the network itself.

CRYP2NOVA

Archived copy · cryp2nova.com

Mixin Domain

Mixin Domain is a distributed ledger to provide assets for the Mixin Kernel. The assets may be those on Bitcoin, Ethereum or any other blockchains, even central organizations like banks.



- Mixin Kernel, the ABFT DAG.
- Mixin Domains, the distributed gateway to provide assets for Mixin Kernel.
- Domain Extensions, could be smart contracts, trusted application, etc.
- Trusted external sources, e.g. Bitcoin blockchain, bank API.

Archived copy · cryp2nova.com

Kernel System Calls

Mixin Kernel offers some system calls to communicate with Domains, and it's the only way the Kernel and Domains can exchange state. The system calls are defined as standard JSON-RPC interfaces.

JSON-RPC is a stateless, light-weight remote procedure call (RPC) protocol. It is transport agnostic in that the concepts can be used within the same process, over sockets, over HTTP, or in many various message passing environments. It uses JSON (RFC 4627) as data format.

Currently Mixin Kernel only implements the standard HTTPS transport for the protocol, and the available calls are listed below.

`kernel_registerDomain`

Register the domain and waiting for the Kernel approval to connect. The call can also update the domain nodes. The registered domain will be forced to form a XIN stake based network between the domain nodes and the Kernel as a whole.

The domain registration is a governance behavior, and should relate to the domain nodes XIN stake. In the future, we hope to implement a more automatic domain management policy in Mixin Kernel. The upgrade policy should always be governed by all Kernel Nodes and XIN holders.

Archived copy · cryp2nova.com

Parameters

1. `UUID` - A unique UUID that represents the domain among all other domains.
2. `Array` - Array of domain nodes' transparent public keys.

```
params: [“c6d0c728-2624-429b-8e0d-d9d19b6592fa”,
[“4b7a842ce6050c99450dc30b4e848c4eaffd33915653b472d900f47
d11722058”,
“b3aef7b3a998a593c157103d20f9cb17bdbd535f304b17c862e3b35b
108faeb8”]]
```

Returns

`String` - Indicate the registration request state, the value is one of `invalid`, `pending`, `denied`, and `approved`.

Note that, all Kernel System Calls should be forwarded to *b* known Kernel Nodes to ensure delivery.

Standard Domain Interfaces

A domain can only be registered to the Mixin Kernel if it implements all the Standard Domain Interfaces.

`domain_getKeyDerivationFunction`

Get the domain specific asset key derivation function, which is one of some key derivation methods in Mixin Kernel, and could be upgraded with governance.

The supported methods may also be extended to some sandboxed VM languages such as solidity.

Archived copy · cryp2nova.com

Parameters

1. `UUID` - The global unique asset ID in the whole Mixin Network.

```
params: [“c6d0c728-2624-429b-8e0d-d9d19b6592fa”]
```

Returns

`Object` - The function name and parameters.

1. `method: String` - The function name, one of the predefined derivation function names in Kernel.
2. `params: Array` - The parameters should be used relative to the method.

`domain_associatePublicKey`

Associate a Mixin public key to the domain for an asset supported by the domain. The public key and domain asset association is the magic that will associate an external asset to the Mixin Kernel.

After public key associated with an asset, it will get an asset specific public key, e.g. Bitcoin public key.

Whenever the Bitcoin blockchain has an output to this public key, the domain will create a transaction to the Mixin public key.

This works because the Mixin Kernel and the Mixin Domain is also a Proof of Stake network. Besides the XIN collateral, there are also additional Intel SGX enforcement for all related functions.

Archived copy · cryp2nova.com

After the domain create the asset transaction to the public key, the asset will be locked by both the Mixin Kernel and Mixin Domain. This result in a corresponding asset lightning transaction in Mixin Kernel.

Parameters

1. `String` - The Mixin public key.
2. `UUID` - Unique asset ID within the whole Mixin Network.

```
params:
[“4b7a842ce6050c99450dc30b4e848c4eaffd33915653b472d900f47
d11722058”, “c6d0c728-2624-429b-8e0d-d9d19b6592fa”]
```

Returns

`String` - The asset specific public key associated with the Mixin public key.

`domain_unlockAsset`

Unlock the asset and transfer out to external sources, this is similar to the withdrawal action on a crypto asset exchange.

The operation to unlock is somewhat similar to the associate function, it must be signed by both the Mixin Kernel and Mixin Domain to make it a valid snapshot acceptable by the network.

Parameters

1. `UUID` - Unique asset ID within the whole Mixin Network.

Archived copy · cryp2nova.com

2. `String` - External asset specific public key.
3. `String` - The amount of asset to unlock.
4. `String` - The fee for external source transaction.

```
params: [“c6d0c728-2624-429b-8e0d-d9d19b6592fa”,
“15SdoFCiwaoUN4grnhPCoDWxWLcY6ZT68V”, “12.345678”,
“0.0005”]
```

Returns
`String` - The external sources transaction identifier, e.g. transaction hash.

The above three Domain Interfaces are mandatory for all domains to be approved by the Kernel. They communicate through the Intel SGX trusted transport layer, and all encrypted private keys are securely duplicated in all Kernel Nodes and Domain Nodes.

Domain Extensions

With a transaction only purpose Mixin Kernel, and Mixin Domains as assets provider and gateway to external blockchains or any other sources, Mixin has become the most sophistic and high performance distributed ledger to almost all digital assets.

However, people need smart contracts, which have been made popular by Ethereum. We allow Extensions to Mixin Domains, something similar to smart contract but with higher robustness, capability and performance.

Archived copy · cryp2nova.com

Domain Extensions are programs running in the Domain Virtual Machine secured by the Secure Enclave in Intel SGX, a popular and secure Trusted Execution Environment.

Due to the possibility to run the “smart contract” in a single computation unit, Domain Extensions can achieve many goals which are almost impossible in something similar to Ethereum.

1. Much higher performance and lower latency which is only limited by the hardware.
2. Non-deterministic transactions, e.g. trustable random number.
3. Interact directly with trusted external sources.

Besides these trusted applications, it’s also possible to run other popular distributed VM, e.g. Ethereum or EOS.

CRYP2NOVA

Archived copy · cryp2nova.com

Attack Resistance

Due to the PoS and distributed nature of both Kernel and Domain Nodes, and enforcement by Intel SGX, the keys are almost guaranteed to be safe from leaks.

Because of the highly distributed key duplication and secret sharing mechanism, the encrypted private keys are also guaranteed to be safe from loss.

Ideally, each asset should have many different distributed domains, these domains are governed by the Kernel and securely enforced by Intel SGX.

The associated keys can only be accessed from where they were generated in the Domain, further improving the degree of protection.

The Kernel will balance the assets in different Domains constantly to further prevent the asset loss in the event of an almost impossible private key leak or loss in different domains.

We will prove that Mixin is safe for digital assets against different possible attack vectors.

To simplify the explanation, only Bitcoin will be used as a sample.

Archived copy · cryp2nova.com

Key Association

Key association is the first step to grant a Mixin public key with Bitcoin access.

Every Mixin public key $M_{\mathtt{pub}}$ will have a Bitcoin public key $B_{\mathtt{pub}}$ associated, how this association occurs and is managed determines the key safety.

$B_{\mathtt{pub}}$ is the public derivation of Bitcoin private key $B_{\mathtt{priv}}$, so how $B_{\mathtt{priv}}$ is generated defines the $B_{\mathtt{pub}}$ correctness.

$B_{\mathtt{priv}}$ is generated purely by the Mixin Domain itself, and it will transfer part of it to the Kernel to keep it by *(t-n)*-threshold secret sharing scheme. If the domain is trustable in this procedure, the association is absolutely secure.

Intel SGX will enforce the domain trustworthiness, and even when Intel SGX itself is not safe, which is almost impossible, the following parts in this paper will prove that the Bitcoin asset will also be secure in Mixin.

Deposit Attack

Deposit is the action when external assets flow into Mixin Kernel, this is the first step when some BTC joins Mixin.

Since key association is proved secure, and all Mixin Domains are governed by Mixin Kernel, if some BTC

Archived copy · cryp2nova.com

successfully submitted to the Kernel, it will be guaranteed to the correct $M_{\texttt{pub}}$.

All Bitcoin deposits will also require a large enough domain finality threshold, e.g. there must be at least 12 Bitcoin confirmations before the system accept the asset.

In this way the system has enough time to detect fraudulent domain action and will punish it without any Bitcoin loss.

The domain mandatory Intel SGX requirements will improve this further.

Fraudulent Domain or Key Leak

The Mixin Kernel constantly balances the assets across all Domains according to their behavior and collateral amount. If a domain is compromised or hacked, the leaked key will only cause partial Bitcoin loss.

Also, Intel SGX will prevent fraudulent Domains from existing and keep hackers away in most cases.

Further more, Kernel and Domains will always load most Bitcoin into a multi signature $B_{\texttt{mpub}}$, this is almost impossible get hacked, especially when correctly and transparently distributed.

Archived copy · cryp2nova.com

Damaged Domain or Key Loss

Just like the fraud domain issue, domain damage or key loss will only affect a few Bitcoin assets.

Since Mixin Governance will ensure the Domain is correctly implemented as a distributed system, it's almost impossible to have the domain damaged as a whole.

Compare to Exchange

Exchanges or other kinds of central managed Bitcoin solutions typically store most BTC in their cold storage.

Cold storage refers to private keys which are never exposed to the Internet and managed by several people in the same firm.

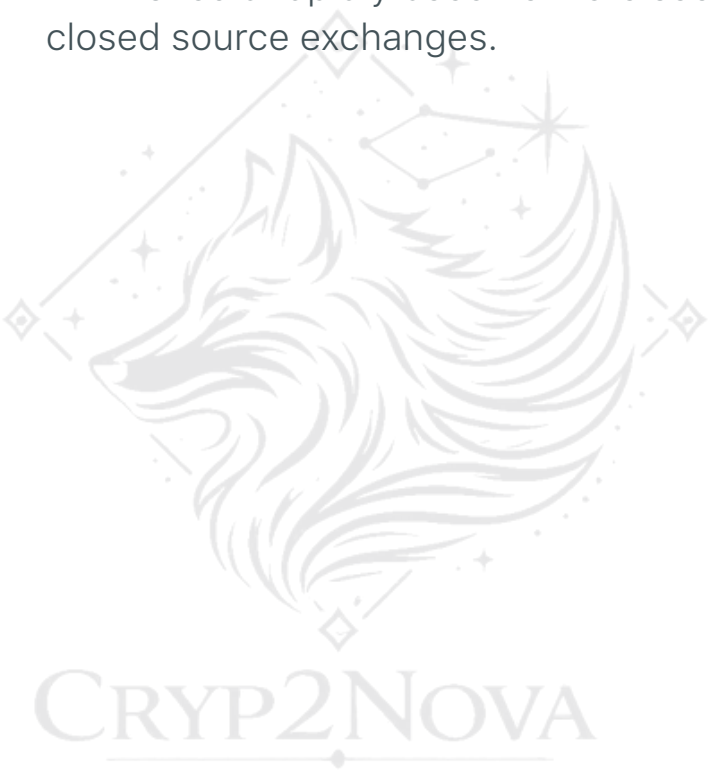
In terms of security, if both Mixin and Exchanges implement the solutions correctly without any bugs, Mixin should be considered much safer and trustable., because Mixin multi-signature $B_{\texttt{mpub}}$ is guaranteed to be managed by many different parties that are unknown to each other, while exchanges have their keys kept by their own people who are much more easily capable of colluding.

Hackers aside, exchanges may have the chance to steal the money by themselves. This is much harder or even impossible on Mixin.

Archived copy · cryp2nova.com

Further, since exchanges are almost all closed source systems, they often have bugs which are not discovered until a hack occurs.

Since Mixin is transparent, the code is open to all users and developers to review and improve, in the same way that Linux is thought to be more secure than Windows, Mixin should rapidly become more secure than any closed source exchanges.



Archived copy · cryp2nova.com

Governance

We try our best to make Mixin Network simply work without any heavy-handed governance, but there are still situations that may require intervention.

XIN is the only stake to determine how the governance work on all the Mixin problems. The vectors that can be voted to governance are listed.

1. Amount of Kernel Node penalty, mainly assessed when double spend, or fraudulent assets are detected.
2. Asset and Domain registration, determine which assets are to be added to the Mixin Kernel. This may be programmed automatically in the future.
3. External asset assurance, e.g. how to recover when Bitcoin forks after the domain finality threshold.
4. Kernel development and upgrade. Determine some policy in the Mixin Kernel specification and upgrade procedure.
5. Community development, vote on community issues if critical.

Archived copy · cryp2nova.com

XIN - The Token

XIN is the sole token used by many services in Mixin, including full node collateral, DApp creation and API calls.

To join the network as a full node, one must pledge at least 10,000 XIN token to establish initial trust.

Every new act of DApp creation will have a one-time cost in XIN, the amount of which is determined by the resources the DApp claims to consume. The Mixin API calls from DApps may cost some XIN well, depending on the call type and count.

All XIN penalties and fees charged by the network will be recycled to the mining pool.

1,000,000 permanent total XIN token is issued to the world at one time, and 400,000 of them have been successfully distributed to holders from 25/11/2017 to 25/12/2017 with rate 20 EOS/XIN.

50,000 XIN have been distributed to early Mixin Messenger adopters. 50,000 XIN are reserved for the development team.

The remaining 500,000 XIN will be the incentives for all Mixin full nodes and light nodes.

Archived copy · cryp2nova.com

Conclusion

We have proposed the Mixin Network as a multi-layer distributed network. The core layer (Mixin Kernel) is a highly distributed transactional network designed according to the ABFT directed acyclic graph. The Mixin Domains layer is quite extensible without any overhead to the Mixin Kernel performance.

We also have a thorough security proof that when managing external blockchain assets, Mixin is secure for daily usage compared to almost any existing cold storage solutions.

The most important thing is that Mixin isn't inventing any new things, and all technologies described in this paper have been used as modules in existing mature projects.

The Mixin Messenger app has proved that this paper is feasible to be implemented in real world, unlike most other projects that have beautiful new theories but no evidence that their work can actually be implemented in the real world.

Archived copy · cryp2nova.com