Mixin Network

Build the largest and most developer-friendly mobile blockchain network, connect all existing blockchains with unlimited throughput.

Technical white paper

Contents

Motivation

Blockchain and cryptocurrency news have become more familiar to people, but it's still difficult to get into these fancy things, even for software developers.

Most blockchain projects focus on the distribution factors and secure key management. However these all lead to slow transactions, private keys loss and difficult understanding. And it's nearly impossible to deploy these distributed nodes on mobile devices, the most popular computing devices.

Despite their effort on the distribution dream, we have noticed the reality that even the most distributed blockchain consensus algorithm leads to the control of several large pools. Consider the BCH hard fork to BTC.

Some popular blockchain projects have or plan to choose some not so distributed consensus algorithms by design, Ethereum is migrating to PoS and EOS is implementing DPoS. This effort may improve the transaction throughput, but that's all.

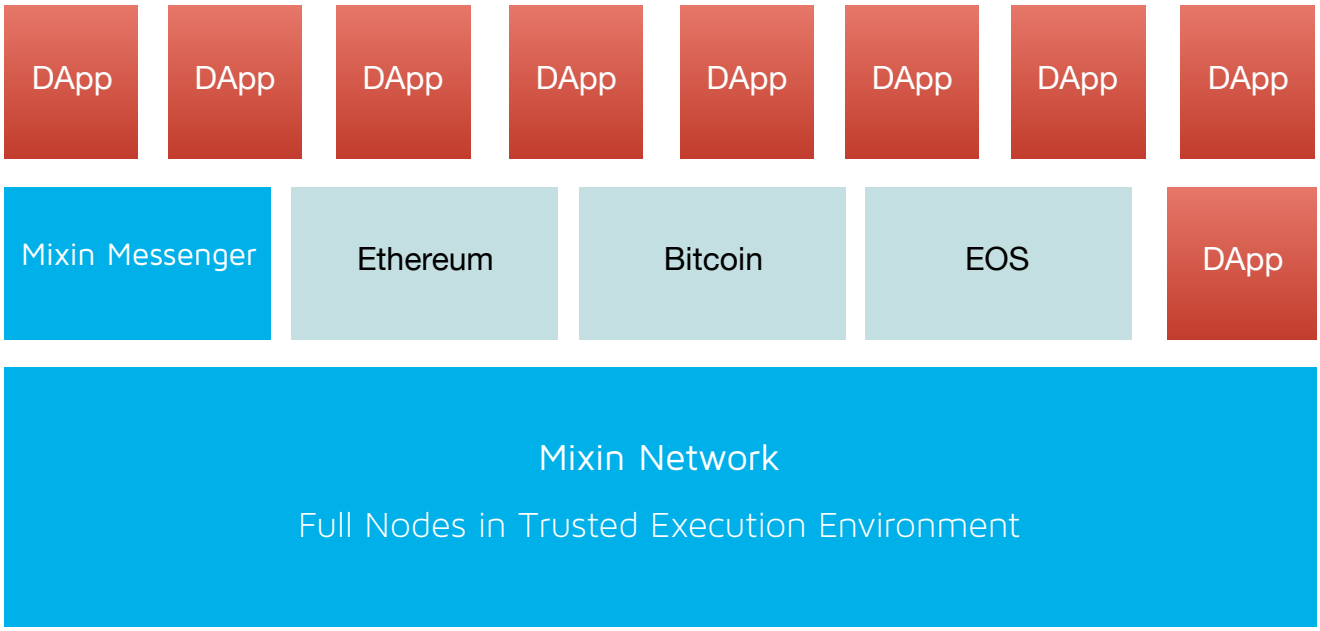
Still, people have to manage fancy private keys and lose them, pools and whale nodes will fork the network endlessly without effort, developers try their best effort to develop some new tokens, and people have no proper way to use the nodes on their mobile devices.

Design

Mixin is an effort to find a balance in distributed network and traditional server clusters, make some tradeoffs to combine the pros of the two together.

- Limited and trusted full nodes with guaranteed data transparency and consistency.
- Zero-knowledge proof and free transactions with high throughput and low latency.
- Inter-blockchain communication protocol to connect all popular blockchain networks.
- Non-deterministic transactions and interact directly with trusted external sources.
- Phone number and PIN based account model for easy mobile use.
- Secure and end-to-end encrypted messaging channel to reach every account for notifications.
- Developer friendly to facilitate all Linux libraries and programming languages.
- The largest mobile blockchain network effect should prevent forks.

To accomplish these goals, we designed an unique blockchain model that relies on Trusted Execution Environment technology and relationship, while the consensus algorithm mainly acts as the guarantee for data replication, and the mobile nodes will acts as validators to do runtime attestation of the full nodes.



As illustrated in the figure above, the fundamental of Mixin network is some trusted full nodes run in the Trusted Execution Environment.

All Mixin full nodes are fully trusted because they can verify the identity of all other full nodes and validate the code they run through TEE attestation at runtime.

Mixin full nodes accept transactions and participate in the network's consensus algorithm. Due to the code validation, only one node should execute DApp code to achieve high throughput and low latency.

All sensitive components of the network must run inside the Trusted Execution Environment and are responsible for protecting security and privacy, for maintaining data transparency and consistency.

End-to-End Encryption Messaging

Mixin uses the sender key of Signal protocol to manage all conversations, despite direct message or group chat.

The protocol is client based, so the server only acts as a proxy of the messages, and due to the strong end-to-end encryption feature, no one could inspect anything from the proxied messages, even the Mixin full nodes.

All messages will be permanently deleted on the servers once read by all the recipients in the conversation.

Photos, videos and all other attachments are also encrypted with random AES key before uploading to our cloud storage. Then the client will transfer all the meta information, such as thumbnail, AES key to the recipient with Signal sender key encryption.

As Mixin is using the mature Signal protocol and open source library as the messaging protocol, we won't dig into the technical details of the specification in this white paper.

Mobile and PIN Based Identity

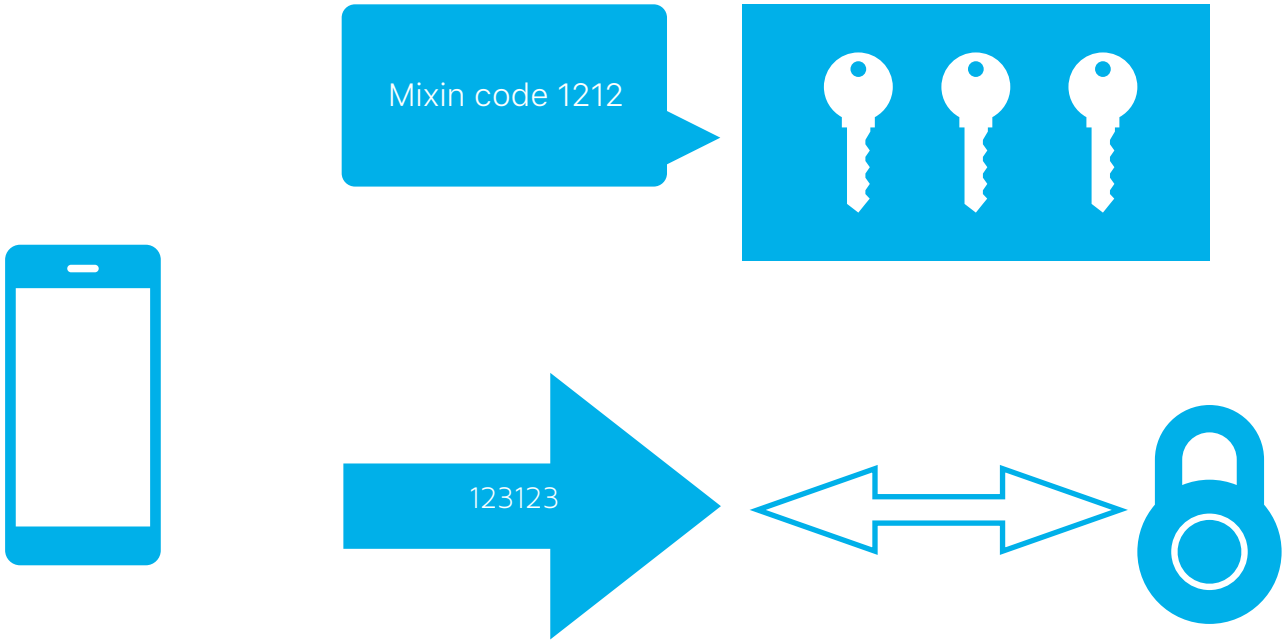
The obstacle that prevents people from using blockchain is not the performance, it's the identity or account management procedure.

All popular blockchain networks require people to obtain and manage at least one private key to keep an identity. This is too complicated, it's not a bit but hundreds of times more complicated compared to username and password solution.

As all existing blockchain data are open to the world, to use an username and password solution, people are still required to manage a complicated password to keep account secure, think about BTS or EOS.

Thanks to the zero-knowledge and secure execution environment in the Mixin network, we are able to design a much simpler identity solution that's based on phone verification code and PIN.

People just need a phone number and remember a six digit PIN to keep an identity, even easier than username password solution, without complicated private key but comparable security level.

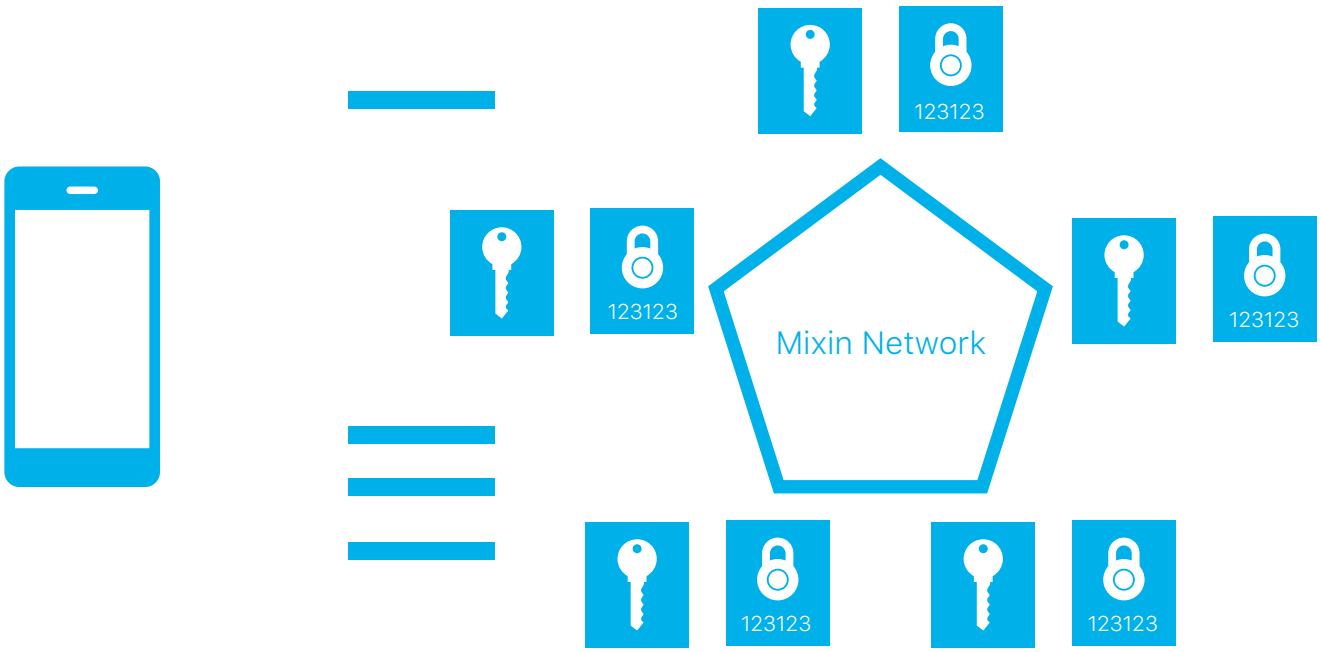


While the phone number verification process to transfer private keys ensure easy phone migration, the 6-digit PIN can be replaced by Touch ID or Face ID on supported mobile phones, this improves the user experience to another level.

A typical BTC transaction should take as long as one hour to confirm, the fee is also too high to send micro-payments. And the public blockchain data make transaction privacy nearly impossible.

To overcome the Bitcoin problem, with the identity procedure above, we designed a cross-chain transaction network similar to the Bitcoin Lighting Network or the Ethereum Raiden Network.

The underlying technique of Mixin PIN identity is still private key management, but secured and made easy by the Mixin zero-knowledge trusted execution network. So it's feasible to treat this as a smart contract like Lighting Network to manage BTC or any other blockchain assets.



After assets from other blockchains come in to the Mixin Network, whenever a Mixin user start a BTC transaction to another user in Mixin, the server won't do any real transactions on the Bitcoin blockchain, instead it just managed their balance numbers in the Mixin blockchain, which is as fast as general SQL database operations.

XIN - The Token

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

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

Every DApp creation will cost some XIN for one time, the cost is determined by the resources the DApp claimed to consume.

The Mixin API calls from DApp will cost some XIN depends on the call type and count.

All the XIN fees charged by platform will be burned to increase the existing XIN tokens value.

This means normal users won't get charged to use the service while only DApp developers are charged, however, the DApp may charge users for its service.

1,000,000 permanent total XIN token is issued to the world at one time, and to make the calculation easier, the Mixin Messenger will mainly use milliXIN as the main currency symbol. We abbreviate milliXIN as MIX, that's the same thing as one thousandth XIN.

Conclusion

Mixin network has unlimited throughput, easy and familiar account model for people, ability to connect and use all currencies on any existing blockchain networks.

Besides the underlying Mixin network, we are building the Mixin Messenger as the first DApp and entrance to it, all code are open sourced to give the developers an overview of how to develop on Mixin.

Treat Mixin Network as the open Android ecosystem, all existing blockchain networks as different phone manufactures and countries, the Mixin Messenger acts as the Google Play role to provide DApp discovery for users, easy notifications and payments for developers.

With nearly 1,000,000 pre-registered users, Mixin network welcome all developers to develop or port their existing app to the platform, with familiar development environment.