ChainX | Light Paper

ChainX:

Trusted and Scalable BTC Layer 2 Network

2020.12.31

ChainX

Introduction

Almost all transactions on the Internet were heavily dependent on banks and financial institutions as third parties to process electronic payments before Bitcoin was created by Satoshi Nakamoto, and the shortcomings are obvious: financial intermediaries increase the costs, unwanted threshold on the transaction size, and potential financial losses due to unexpected refund requests by customers over some goods and services that cannot be returned. Fortunately, a new kind of peer-to-peer electronic payment system represented by Bitcoin can solve the above-mentioned problems.

September 2021 saw Bitcoin officially become the legal tender of El Salvador, and in October, its market value shot up to 1.217 trillion dollars, ranking eighth among all types of global assets (including listed companies, precious metals, cryptocurrencies, and ETFs), surpassing Facebook and Tesla, and will soon exceed silver in terms of market value in the short term. This growing trend is expected to continue as more institutions and individual investors come to know it and jump on the bandwagon.

However, Bitcoin stops short of serving any substantial functions when it comes to large-scale payments due to limitation imposed by block size and block generation. Though crowned as “digital gold”, it is not Turing complete, with its scalability still restricted.

Therefore, ChainX rises to the challenge by establishing a trusted and scalable BTC layer 2 network that can improve both the payment speed and the function expansion of Bitcoin. BTC trustworthiness in the layer 2 network is built up through ChainX’s custodial and non-custodial modes which ensure BTC security; Dapps in layer 2 greatly improve the throughput of Bitcoin transactions and further lower transfer fees. At the same time, BTC smart contract enabled by ChainX also enriches the application ecosystem.

There are two ways for ChainX to do this: the custodial mode and the non-custodial mode.

How does ChainX build up BTC trustworthiness in layer 2 network?

Custodial Mode

In custodial mode, chain-crossing is a process where assets are mapped onto the target chain while remain locked in the original chain. It also applies the other way around that assets are withdrawn from the target chain, and automatically unlocked in the original chain. Assets do not disappear in the original chain, but are managed by multiple parties in a centralized manner through the light node protocol. There are two custodial solutions in ChainX: V1.0 multi-signature custody scheme and V2.0 threshold signature custody scheme.

V1.0:
Multi-signature custody Scheme

In the V1.0 multi-signature custody scheme, the initial trust nodes are selected from the best performing nodes in the ChainX testnet, with subsequent successors recommended jointly by the council and the predecessors. Two multi-signature addresses or contracts, one cold and one hot, are generated in each node renewal, with funds being transferred from the old addresses to the new ones. Users have full access to real-time inter-chain asset issuance and reserves, which eliminates the possibility of misappropriation and embezzlement by individual node.

When a user sends a transfer from his BTC account to the multi-signature custody address, by adding his ChainX address to the Note, he can cross BTC onto ChainX which issues the equal amount of X-BTC. When withdrawing, after securing signatures of multiple parties, X-BTC will be burnt with the corresponding amount of BTC transferred from the multi-signature account to the user account.

V1.0:
Multi-signature custody Scheme

Inter-chain deposit

ChainX runs the Bitcoin light nodes, and Relay transmits the Header in real time to keep the longest chain updated. When a user sends a transfer to a custodian's hot address and adds the user's ChainX address in hexadecimal format to the OP_RETURN as Note in the transaction, only transfer bridge with the OP_RETURN Note can identify the transaction with the user. Monitoring the Bitcoin network, Relay submits Tx, Proof, OP_RETURN and related information to the transfer bridge after the block of the transaction is confirmed by the original chain, then the transfer bridge verifies the Tx and the OP_RETURN Note, if both valid, X-BTC will be issued to the ChainX address attached to the OP_RETURN Note.

Inter-chain withdrawal

A user initiates a BTC withdrawal in the ChainX network, which prompts the recording module in the ChainX transfer bridge/gateway into action by locking the corresponding amount of X-BTC and recording the user's application information that is associated with the user's ID. Meanwhile the custodian obtains the information of ongoing withdrawal at a regular basis, based on which the BTC withdrawal transaction is formed and submitted to the ChainX Bitcoin transfer bridge and then the corresponding withdrawal record is locked, and finally other custodians co-sign this transaction. Relay submits the transaction to the BTC network after signing is completed; if confirmed, Relay then submits the transaction and the proof path to the transfer bridge which verifies the Tx. If valid, the corresponding withdrawal record will be closed and the locked X-BTC will be burnt.

V2.0:
Threshold Signature Custody Scheme

What remains the same with version 1.0 is that BTC withdrawal still requires multiple signatures of the custodians to complete the asset transfer. What differs is that in 2.0, we use the threshold multi-signature technology to replace the traditional multi-signature method.

Threshold signature is a distributed multi-party signature protocol. Each party signs a transaction in a distributed and collaborative way on the basis of their private key share. If the threshold share number is met after combination, the final verifiable signature is generated.

ChainX adopts the Bitcoin Taproot technology, and uses the Schnorr signature technology and MAST (Merkelized Abstract Syntax Tree) to pave way for the implementation of threshold signature. Schnorr signature aggregates public keys of multiple users into one to generate the corresponding aggregated signature, based on which, the MAST protocol combines the multisig logic of sr25519 to achieve threshold signature.

Game theory (only involving small sums)

The threshold signature protocol uses the small-sum game theory to manage private key custodians. With PCX, the native token of ChainX as collateral, the collateral token competitors are BTC threshold signature custodians according to the small-sum game theory.

Custodian's rewards

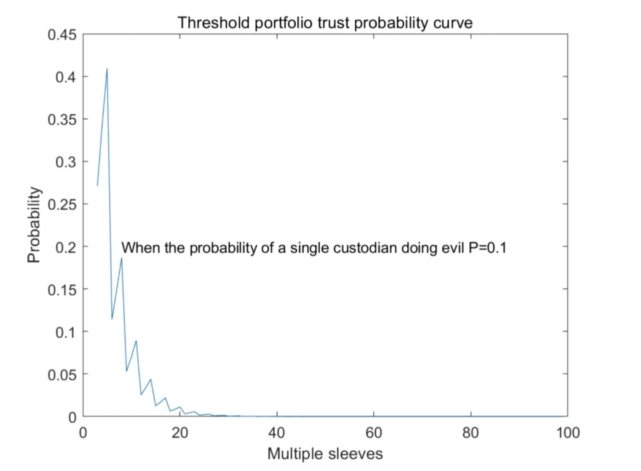
Custodians benefit from service fees, and 5% of the revenue from treasury will also be rewarded to outstanding custodians.

Let’s assume the probability of a single custodian attempting malicious deeds is P, then the probability of over m custodians doing evil deeds among n nodes (m/n=1/3) is:

$$\sum_{m=n/3}^{n} C_n^m * p^m * (1-p)^{n-m}$$

V2.0:
Threshold Signature Custody Scheme

When P=0.1, as the number of nodes increases, the resulting probability curve is as follows:



When P=0.1, the probability of evildoing by n custodians decreases rapidly as n increases, and approaches zero when n>20. In other words, in a single round 1 BTC as collateral can cross 1 BTC at most onto other chains; however when n>20, 1 BTC collateral can cross over 10,000, which solves the problem that the BTC market value far exceeds its cross-chain collaterals. But the premise is to ensure that the probability of a single custodian doing evil is less than or equal to 0.1.

Non-custodial mode

In custodial mode, chain-crossing is a process where assets are mapped onto the target chain while remain locked in the original chain. It also applies the other way around that assets are withdrawn from the target chain, and automatically unlocked in the original chain. Assets do not disappear in the original chain, but are managed by multiple parties in a centralized manner through the light node protocol. There are two custodial solutions in ChainX: V1.0 multi-signature custody scheme and V2.0 threshold signature custody scheme.

What is Lightning Network?

The Lightning Network is a new protocol layer based on Bitcoin that uses cutting-edge smart contract technology to achieve faster transaction throughput than VISA, while retaining the point-to-point nature of the Bitcoin protocol. It has creatively designed two types of trading contracts: RSMC (Revocable Sequence Maturity Contract) and HTLC (Hashed Timelock Contract). RSMC solves the problem of one-way flow, and HTLC, across-node transfer. The combination of these two types of transactions constitutes the Lightning Network.

The Lightning Network reduces Bitcoin transaction time and fees by cutting the number of transactions that need to be permanently stored on the chain. Instead, transactions are stored in the "payment channel" of the smart contract, and completed between two parties outside the chain. Transaction balance in the channel is constantly broadcast to the Bitcoin network, with settlements conducted safely on the chain.

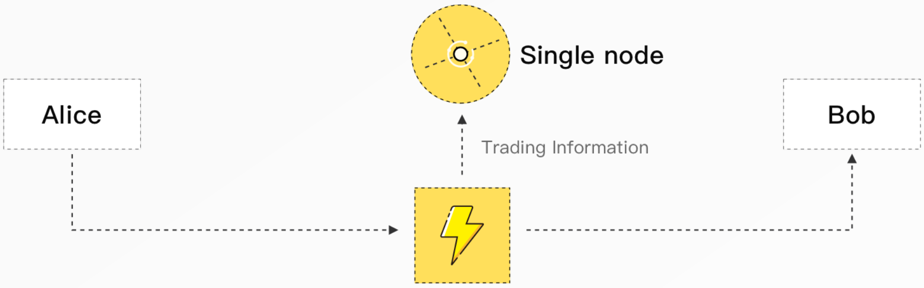
X-Lighting

X-Lightning is a standard-compliant implementation of the Lightning Network Protocol on the ChainX mainnet. It moves the off-chain bookkeeping to the distributed blockchain network, solving the problem of individual node failure and addressing the concern of lacking transparency in the off-chain ledger of the Lightning Network. X-Lighting helps implement smart contracts on the Lightning Network via ChainX. In addition, X-Lighting adopts multi-signature other than the existing double-signature to enhance the performance of Lightning Network in special areas.

Non-custodial mode

How does X-Lighting address individual node failure in the Lightning Network?

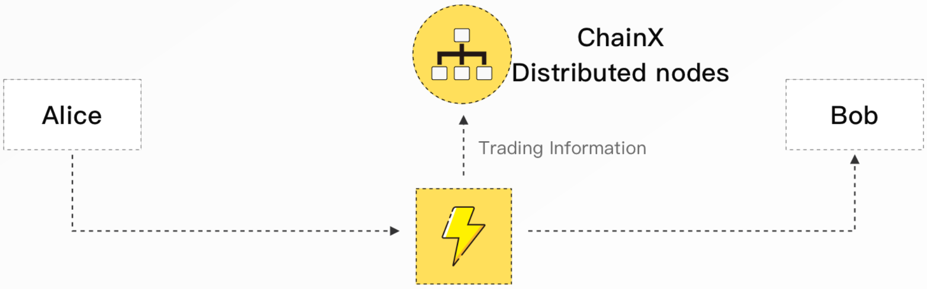
In the past, a two-way payment channel was formed by the two trading parties according to RSMC, and detailed transaction information in the channel would be recorded in the off-chain ledger. However, the fact that bookkeeping is done off-chain and by third-party nodes is problematic, leaving the system prone to individual node failure and node evil-doing.



Transaction via Lightning Network State Channel

Both parties of the transaction conduct a certain currency transaction through the Lightning Network, and the transaction information is recorded in the third-party account book under the chain. This can lead to problems such as single node of failure or evil.

We solve these problems by recording the transaction information on the ChainX chain and switching to decentralized bookkeeping.



Transaction via Lightning Network State Channel

Both parties of the transaction conduct a certain currency transaction through the Lightning Network, and the transaction information is no longer recorded in the off-chain ledger, but on the ChainX block, which solves the single-node failure problem of off-chain accounting.

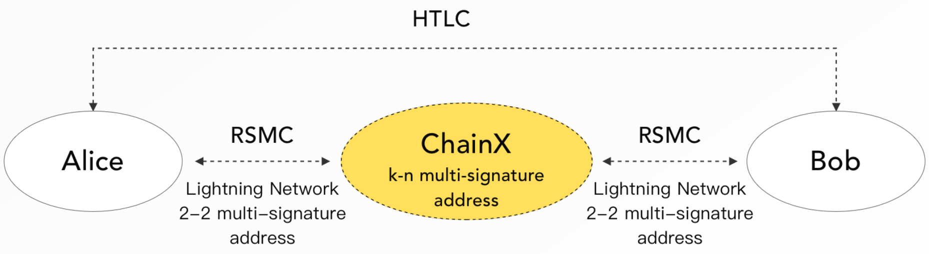
Non-custodial mode

How does X-Lighting achieve cross-node transfer?

Assume A and B want to transfer Bitcoins to each other, but they are not connected by any state channels directly. In the past, they could resort to multiple routing nodes to settle the transaction(as shown in the figure below).
A⇔C⇔D......N⇔B
But the truth is A and B may not even be able to find such a connected routing path before the Lightning Network users reach a certain scale. Even if they do, this solution involves the use of complex routing algorithms, with intermediate nodes charging variously according to their different payment channel networks, which further complicates the already intricate transaction fees.

In the face of these problems, ChainX comes up with a solution. First, establish a k-n multi-signature address, which is composed of n well-endorsed and trustworthy nodes on ChainX, then form a 2-2 address between the multi-signature address and the wallet address of each ChainX user on the basis of RSMC of the Lightning Network, and then through HTLC, A and B can transfer bitcoins freely.

More improvements are made to the multi-signature address after the upgrade of Taproot where the Schnorr algorithm linearly aggregates privates keys off-chain to form a threshold signature. Therefore, the multi-signature address can be jointly formed by countless nodes in theory, which further improves the transaction security.



How does ChainX achieve Bitcoin scalability?

ChainX supports the deployment of smart contracts through virtual machines and execution environments such as WebAssembly (Wasm) and EVM, and provides quality development environment for Dapp developers.

Migration at the lowest cost

Deployment on the ChainX chain only requires some simple changes to your existing smart contracts.

Compatibility with common tools and plug-ins

ChainX allows the use of Ethereum-based tools such as Truffle, MetaMask, Waffle, Remix and Hardhat.

Solidity smart contract

ChainX supports Solidity and other programming languages of the EVM bytecode.

Web3RPC and H160 accounts

ChainX is compatible with the Ethereum's Web3 protocol, which enables ChainX to interact with the existing Ethereum accounts and private keys.

Through smart contracts, Bitcoin can achieve instant contract payment and higher scalability on the ChainX mainnet, which in return greatly increases the value of Bitcoin and enriches its functions. ChainX welcomes developers to explore applications surrounding XBTC and LBTC.

The market value of Bitcoin keeps on breaking new highs as it is increasingly recognized by mainstream institutions, paving the way for it to become one of the mainstream means of value store, especially when its price shows a stable upward trend. Against this backdrop, the market has high demands for hedging and leveraging tools for digital asset investment. To cater to the needs, ChainX will gradually take onboard derivatives such as BTC futures, options, synthetic assets and swap agreements. In the future, DAPPs in various fields like gaming, NFT and social media will rely on the ChainX Bitcoin ecosystem to create, develop and prosper.

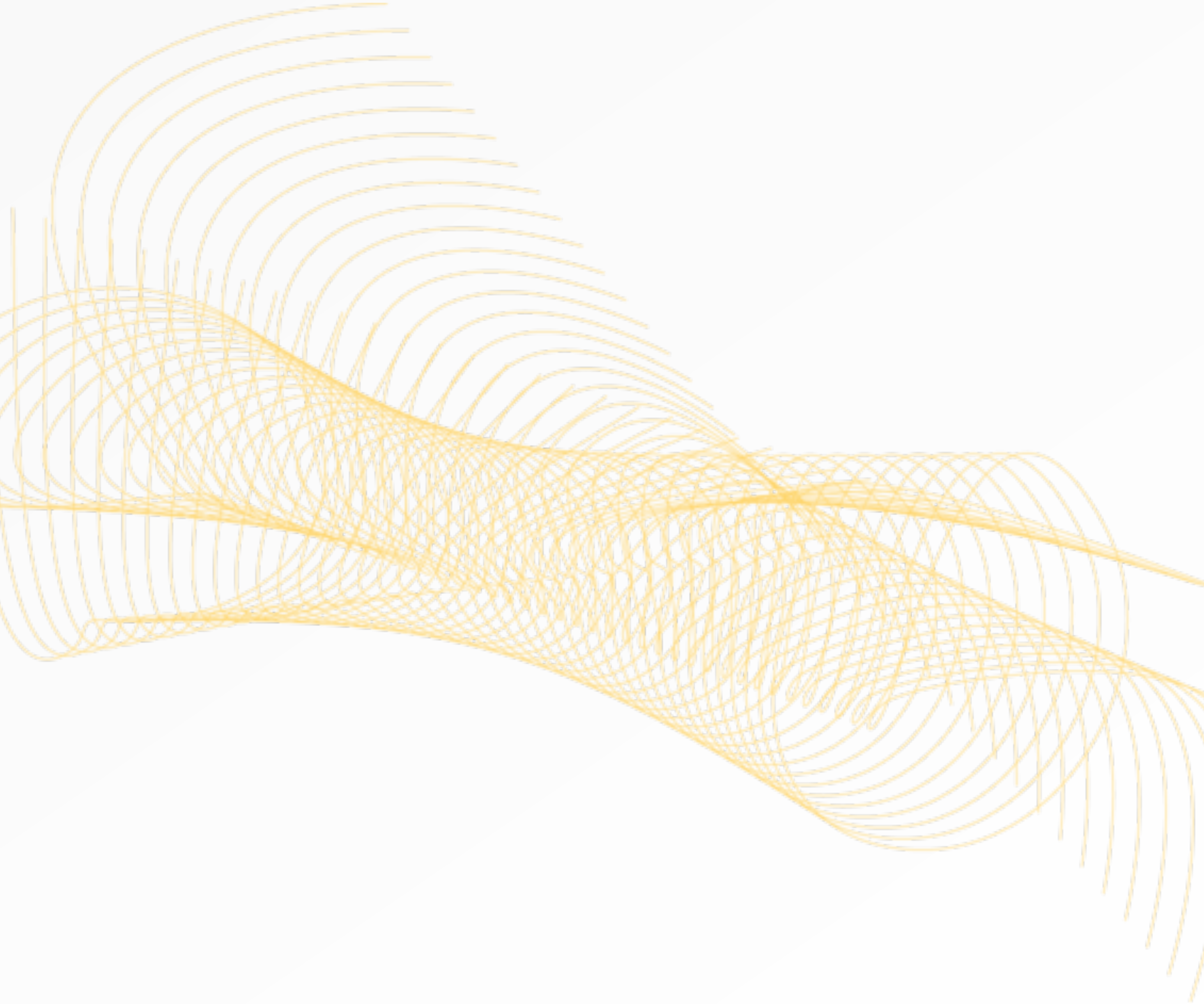
How does ComingChat empower the ChainX ecosystem?

ComingChat is a trustworthy social metaverse. Its mission is to build a metaverse for the entire ecosystem. On the one hand, with the economic structure of Bitcoin, it aims to reshape the digital economy system for billions of people around the world by building a simple, secure, and private global payment system and financial infrastructure. On the other hand, it further strengthens the interaction between the Internet and the real world by serving as a gateway for users to enter the Web3.0 world where a programmable identity system is established with CID as users' digital identity, thus achieving unprecedented interoperability.

ComingChat will provide access to ChainX applications, attracting more Web3.0 users to the ChainX platform.
ComingChat will designate ChainX wallet as the official wallet which supports cryptocurrencies such as PCX, XBTC, LBTC, etc.

Consensus Algorithm

ChainX adopts Polkadot's new consensus mechanism, the "Babe+Grandpa" hybrid consensus algorithm. The most notable feature of this algorithm is that it separates block confirmation from block generation, with the BABE module generating blocks every 6 seconds, and Grandpa making the final confirmation.



Economics

Token

The governance token in ChainX is PCX. The total supply is 21 million, with the output halved every two years.

PCX function

PCX tokens have three purposes: governance, staking and payment.
PCX represents the voting rights on the ChainX network, giving holders the right to vote on the chain's protocols, products, new features, goals, upgrades and maintenance.
PCX holders are incentivized to stake their tokens to protect the network, and at the same time they receive rewards.
ChainX charges transaction fees, for every transaction on ChainX requires computing power, and it is PCX that facilitates the process.

Community Autonomy

To promote decentralized governance of the community, ChainX adopts the Tricameral governance structure as Polkadot does, including a Referendum Chamber, a Council, and a Technical Committee. In addition to that, the concept of X–Association and Treasury is added to further improve the framework of community autonomy.