

# ChainX | White Paper



# The Layer2 platform for Bitcoin

	2
Background	3
Overview	4
Overall Structure	6
Economic system	8
Consensus algorithm	12
Account system	13
Community autonomy	14
Bitcoin financial platform	19
Digital asset gateway	28
Polkadot second-layer relay chain	29
Roadmap	30

Bitcoin, a blockchain-based digital currency with 21 million fixed supply, has seen its value grow from almost zero to \$20,000 in the past 11 years after its birth, which shows the hallmarks of Bitcoin as a trading commodity. Bitcoin was awarded the title of "Digital Gold" in 2017 due to its irreplaceable features like anti-inflation, decentralization, globalization, anonymity and so on.

The meteoric rise of DeFi, Paypal's olive-branch policy to take cryptocurrencies Bitcoin included onboard, the newly-established digital currency exchange by the Development Bank of Singapore, and the ostentatious display of support by Grayscale in buying Bitcoins, events like these are too many to exemplify one by one, but the underlying importance and meaning far exceeds the market value growth from \$4,000 to \$20,000. This indicates that Bitcoin is being re-recognized as a payment method, perhaps only a tip of the iceberg in terms of its full potential. Along with that, there are also macro practices by the financial market: Bitcoin's spillover effect (DeFi), derivatives market, grayscale fund, etc.

The hidden potential of Bitcoin is being tapped and released as it holds the key to the digital currency world and leads towards deeper blockchain breakthroughs. A groundbreaking technological change spearheaded by blockchain technology has gotten underway in recent years, aiming to start another major technological shift after the Internet. Among many, the one that has received the most attention is Bitcoin's Layer 2 solution with extensive research being done on it to expand and enhance the performance of blockchain.

**ChainX is committed to Layer 2 expansion and asset gateway research of Bitcoin, well positioned to provide high-performance transaction trusteeship and interoperability among chains in asset transfer.**

Layer 2 technology is often dubbed as an "off-chain" solution, expanding blockchain networks while retaining the decentralized advantages of distributive protocols. A good blockchain ecosystem requires some changes in the framework to balance security, decentralization, and scalability. That's where layer 2 platform and protocol which reduces the burden on the base layer (root chain) is needed by reassigning part of the data processing of the main chain to layer 2, thereby enhancing the scalability of the entire blockchain network. Blockchain is embarking on an evolving path towards a multi-layered system. The layer 2 expansion looks set to create new "usable" blockchain systems with its influence percolating through other industries, ushering an era where blockchain layer 2 application scenarios payment included will be flourishing without damage being done to layer 1.

**ChainX Asset Gateway, the first project developed on Substrate, works as the asset transfer hub for the Polkadot ecosystem, connecting assets outside Polkadot via its inter-chain messaging protocol, opening transferring routes among multiple chains after success achieved in single ones. It has gradually evolved into Polkadot's second-layer relay chain, routing external mainstream assets including Bitcoin into Polkadot and incubating financial derivatives and services.**

**ChainX, the earliest launched project in polkadot ecosystem, is based on Substrate which is a blockchain framework development platform designed by the Parity team led by Gavin Wood, Ethereum's former CTO. It has universally applied State Transition Function (STF) and modular components to reach consensus in terms of network and configuration. In addition, it conforms to the standards and conventions of the underlying data structure, in particular the Substrate Runtime Module Library (SRML), which allows rapid creation of a new chain. And ChainX attributes a substantial part of its growth and progress to the universal applicability of the Substrate framework.**

ChainX is committed to the research and application of Bitcoin layer 2 expansion, digital asset gateway and Polkadot second-layer relay chain. In terms of governance and operation, ChainX adopts a dynamic asset mining model for safe governance and efficient consensus; in terms of technical implementation, ChainX manages to cross mainstream cryptocurrencies onto chains with different structures through the "light node + trusteeship" scheme and forms a digital asset gateway through its decentralized Bitcoin trusteeship and inter-chain mirroring mechanism to make grounds for transactions of all sorts of cryptos on the same chain; besides, as the second layer of Polkadot, ChainX dissects multi-chain frameworks, builds parallel transfer bridges and facilitates transactions among multiple parties.

The initial version of ChainX is based on Substrate 1.0 and operates smoothly for one and half years. After Polkadot 2.0 was officially released, ChainX spared no efforts to upgrade its mainnet and launched the 2.0 version at the end of November 2020. On the base framework of Substrate 2.0, ChainX 2.0 combines and coordinates various functions like hybrid PoS consensus, on-chain council governance, Wasm virtual machine, native execution of smart

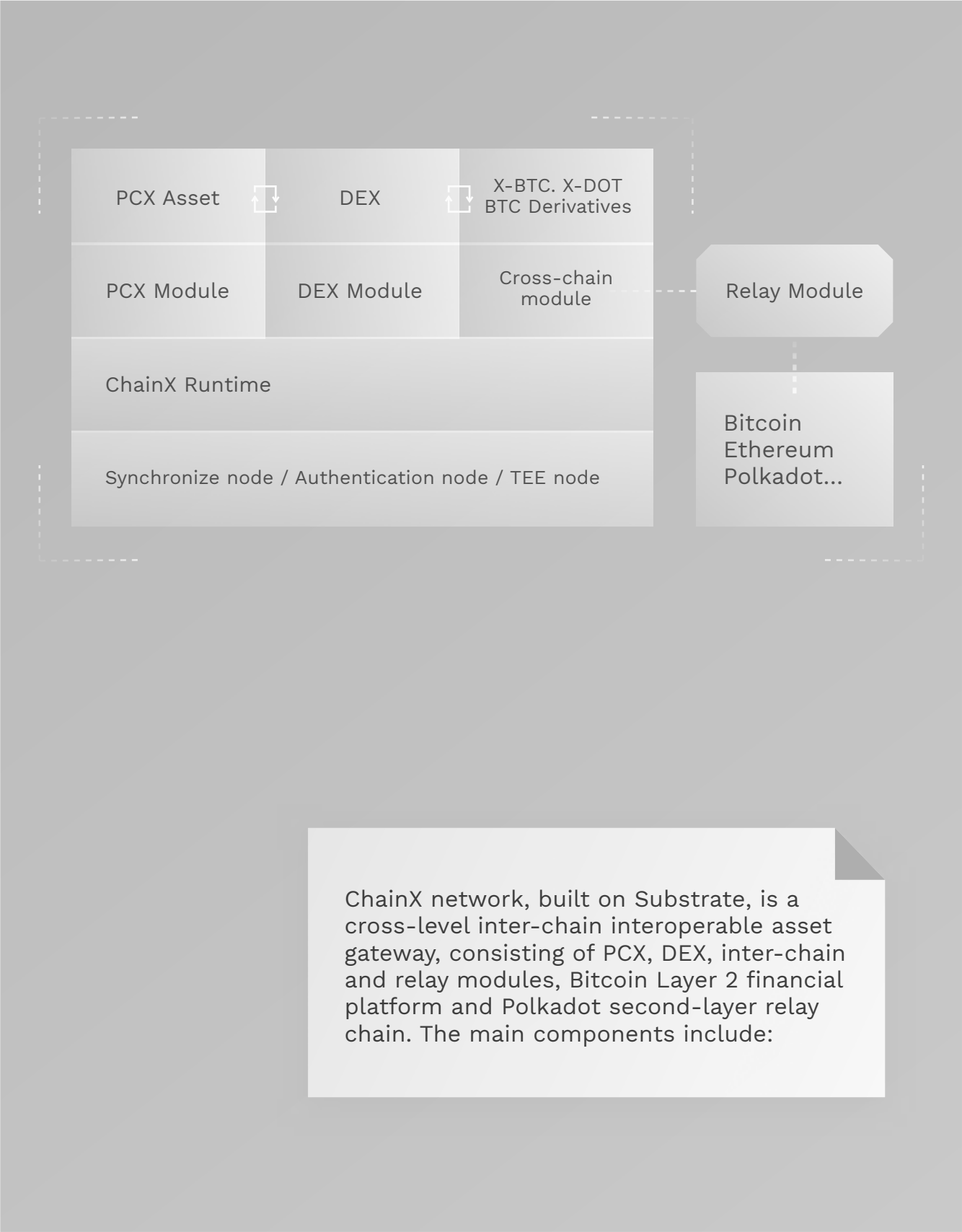
contracts, efficient light-client protocol, Off-chain worker, and multi-signature, what's more it is highly compatible with Polkadot.

"One Asset One Vote" mining model, pioneered by PoS consensus and adopted by ChainX, stipulates that no ICO is planned and assets like BTC, ETH and EOS deposited by users through inter-chain technology should participate in mining at their market value along with the native token. For fear of unfair competition, pre-mining practices and computing power monopoly are prohibited with a fair distribution system of PCX whose generation model follows the footsteps of Bitcoin, gradually halving the supply of new coins. Digital assets crossed onto ChainX can be traded with other tokens on DApp exchanges, associated with Bitcoin financial derivatives and generate fair prices in terms of assets' market value for mining.

The decentralized light-node technology that ChainX currently adopts integrates mainstream digital assets across chains, with Bitcoin standing as a prominent success. In the future, more upgrading and improvements can be expected in the inter-chain technology with added help from methods like independent

trustee, MPC, and homomorphic encryption; more Bitcoin financial derivatives will pop up and flourish; and more mainstream currencies such as ETH, ERC20, EOS, ADA, and ZEC will be connected to ChainX. At the same time, equal importance should be attached to communities where users are encouraged to transfer inter-chain assets among one another and contribute to refine the system, so that Bitcoin is stimulated with constant value flow and DApps equipped with the latest smart contract technology are incubated.

At the era of digital economy, everything is an asset with value which can be traded. Cryptocurrencies represented by Bitcoin are no exception and play an increasingly important role in this new round of international financial and monetary game, which also paves the way for the meteoric rise to fame of the underlying blockchain technology. However, different chains were isolated with no meaningful connections not to mention inter-chain asset transfer, free value flow or low-friction exchange. If the dilemma couldn't be solved, there would be no connectivity and interoperability among chains. To break the stalemate, ChainX expands the layer 2 network of Bitcoin, serves as the digital asset gateway and Polkadot second-layer relay chain to create a safe and stable inter-chain transfer system for assets form all sorts of ecosystems.





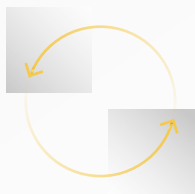
**PCX module**

an operating program based on the native token PCX, it mainly includes functions performed by PCX such as staking, paying fees, on-chain governance, distributing inter-chain mining rewards, and backing Bitcoin financial derivatives. PCX is related to most programs running on ChainX.



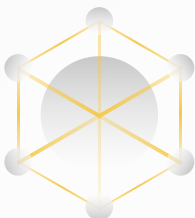
**DEX module**

A cross-asset transaction module, it promotes circulation of assets on different chains while minimizing transaction costs.



**Inter-chain module**

An entering or exiting module for different chain assets and X-Token, it mainly includes an inter-chain transaction verification system, on-chain mintage program, trusteeship program, and deposit and withdrawal program for X-Token.



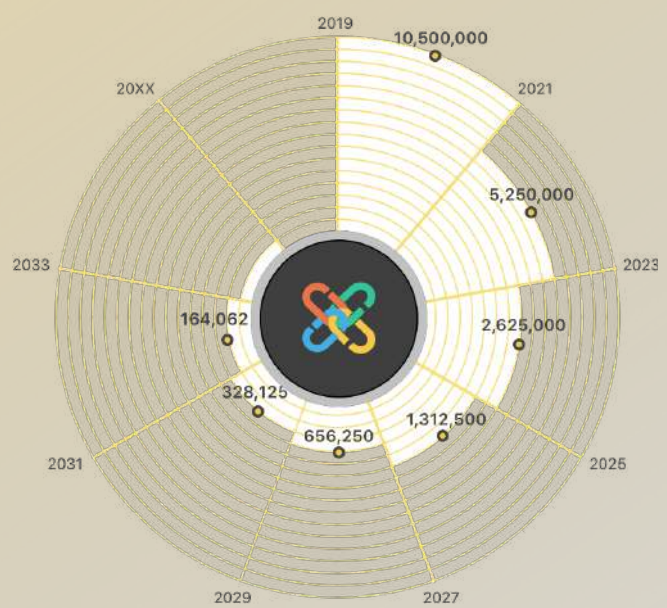
**Relay module**

a window of information exchange and verification between ChainX and outside chains, it mainly includes chain information update program, chain monitor program, and inter-chain information collection and transmission program.



Token generation

The cryptocurrency PCX (P stands for Polkadot) issued by ChainX has 21 million supply in total. In the initial dividend round or the first 210,000 cycles, 50 PCXs are distributed as rewards in each cycle, and 25 PCXs for the second round. 20% of the issuance in the initial round which accounts for 10% of the total goes to the founding team for ongoing development and all the subsequent issuance goes to the community.



Mining

ChainX adopts “One Asset One Vote” mining model which is composed of two forms: inter-chain asset mining and voting mining. All participating parties compete together with PCX as the computing power unit.

Inter-chain asset mining means that various assets such as BTC, ETH, etc. that enter ChainX through depositing, mapping or other means participate in mining with virtual computing power calculated for each. Independent calculating methods are applied to each inter-chain asset such as fixed computing power calculation, market price discount calculation, etc., which will be explained in detail later. The calculation method is mainly determined by community voting. Inter-chain assets are discounted when participating in mining

because PCX as the native token naturally comes with greater mining power, which in return encourages users to hold more PCX.

**Voting mining** refers to voting or staking real PCX to certain nodes to participate in mining.



Computing power

The current ratio of inter-chain assets to PCX in terms of mining power is set at 1:9 which can be adjusted through community voting, which means the maximum mining power of all inter-chain assets is set to 10% to ensure PCX voting mining power greater than or equal to 90%.

ChainX is a PoS system where total computing power consists of PCX voting mining power and inter-chain asset virtual computing power with the system’s security guaranteed by PCX, the more PCX, the better. In addition, as an inter-chain asset gateway, ChainX connects assets from other chains, the more assets it connects, the greater the value. Native assets and inter-chain assets both participate in mining, competing with while reinforcing each other. In order to avoid sudden influx of inter-chain assets overwhelming the system in the early stage, dynamic mining model is adopted to cope with rapid surges of inter-chain assets with a fixed dividend ratio between the two. Changes in mining model are determined by the chain governance referendum.

Calculation formula

Power total = Power real + Power virtual  
Power real = Staked  
Power virtual= sum ( Power c ), c ∈ { X-BTC, X-ETH, S-DOT, ... }  
Power c = Amount c·Fixed  
c·UbiquitousDiscount

The current mining power cap for all inter-chain assets is 10%, that is Power virtual : Power real = 1:9。

When Power virtual : Power real > 1:9 时, the upper limit rule takes effect.  
UbiquitousDiscount = Power real : 9 Power virtual

When Power virtual : Power real <= 1:9 时, the upper limit rule becomes invalid.  
UbiquitousDiscount = 1

Power total : Total computing power

Power real : Computing power by staking PCX

Power virtual: Virtual computing power of inter-chain assets

Power c: Total virtual computing power of inter-chain asset C

Fixed c: Fixed multiplier of unit inter-chain asset C, with current Fixed BTC = 400·PCX

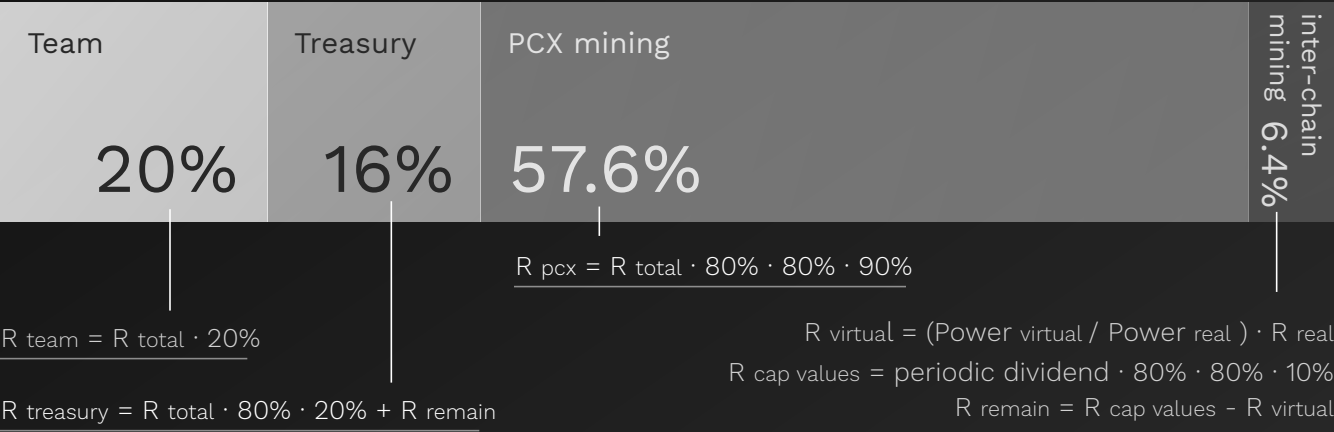
Amount c: Total amount of inter-chain asset C

UbiquitousDiscount: Dynamic discount for inter-chain assets

Income distribution

ChainX's mining income go to four parts: the founding team, the Treasury, PCX mining users and inter-chain asset mining users. The distribution of income can be readjusted with a referendum in future community governance.

The income data in the figure below is calculated based on the hard cap income



Power<sub>real</sub> : Computing power by staking PCX

Power<sub>virtual</sub> : Virtual computing power of inter-chain assets

R<sub>total</sub> : Total amount of PCX generated in a dividend cycle

R<sub>team</sub> : Team income from the initial dividend cycles

R<sub>treasury</sub> : Treasury income

R<sub>real</sub> : Income from PCX real mining power, which is  $R_{real} = periodic\ dividend \cdot 80\% \cdot 80\% \cdot 90\%$

R<sub>cap values</sub> : Hard cap income of inter-chain asset dividends

R<sub>virtual</sub> : Actual mining income of inter-chain asset which goes to mining users

R<sub>remain</sub> : esidual mining income of inter-chian asset which belongs to the treasury

**Team** This part of earnings goes to the founding team to cover ongoing development costs

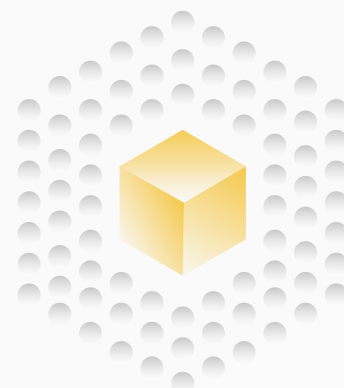
**Treasury** This part of earnings belongs to the Treasury for community development and parachain slot auctions.

**PCX mining users** This part of earnings is rewards to PCX mining users.

**Earnings of inter-chain asset mining are rewards to the mining users.** The specific amount is calculated according to the ratio of virtual mining power of inter-chain assets and real mining power of PCX with the upper limit set at 1:9, if not exceeding the limit, extra earnings go to the Treasury.

Total income is calculated according to the engagement and activities of inter-chain assets and PCX with income for a single node obtained through the proportion of real and virtual nodes, and then income for a user is calculated with regards to the number of votes he or she has cast. When the total number of inter-chain assets surges to the upper limit, a discount on all inter-chain assets will be imposed compounded with the existing ones.

**ChainX adopts the "Babe+Grandpa" hybrid consensus, Polkadot's brand-new mechanism whose most notable feature is to separate block confirmation from block generation with Babe module generating blocks every 6 seconds and Grandpa making the final confirmation.**



In the traditional POW algorithm, the mining power of a single machine is weak, unable to generate blocks independently, which leaves joining a mining pool or building one by one's own the only option and results in only 10 mining pool nodes per chain. The initial POS chain usually has about 7 nodes, and follow-up ones only dozens of nodes. Therefore, blockchain's decentralized advantages are kept untapped with ordinary users unable to become consensus nodes thus having no access to the ledger and having to rely on large organizations.

The number of Consensus nodes in ChainX starts from a few dozen, and gradually grows as the community evolves. At the initial stage, cloud servers are needed to build consensus nodes. Later users only need to download the desktop wallet to generate blocks, but good internet environment and computing power are required, or punishment may be incurred if any block is delayed. The punishment funds will be transferred to the Treasury and future referendums will be held to decide how to use it.

The node's profit model is to obtain 10% mining income of users, and the specific proportion can be modified by future referendums. Node dropout or other malicious behavior will be punished by reducing daily user rewards. The election cycle for each verification node is one hour and nodes will be ranked according to the number of votes. If a node fails to be selected as verification node, becomes a synchronizing node, and heartbeat transactions also need to be initiated with a real node and empty nodes are not allowed. Votes of both consensus nodes and synchronizing nodes participate in the mining reward distribution with the same benefit rate so that the advancement of synchronizing nodes will not be compromised.

**ChainX currently charges a transfer transaction for only 0.0001PCX. As ChainX's performance and throughput gradually improve, fees become lower and can be ignored. In the late stage of network development, additional issuance of chains will gradually slow down and user's mining income mainly comes from transaction fees and various kinds of punishment fees.**

In order to prevent DDOS, users need to pay gas fee for transactions, and the system will charge the corresponding fees according to the complexity of different operations. Users also have different accelerating options according to the network congestion to achieve flexible control. It seems that users need to pay fees which however can be balanced out by the mining income obtained through mining and holding assets in the early stage, enough to meet the trading demands of non-frequent users. Besides, consensus nodes draw transaction fees to the node rewarding pool when packaging and voting users can benefit from it. Therefore, Users can still use the chain "for free" even in this closed system, and most of the mining users can make earnings with only a handful of super-frequent users paying fees. Gas fee is traditionally charged due to low throughput of the chian, which leads to high transaction costs.

PCX mainly has the following uses



**Miner fees**

Pay miner fees, similar to miner fees in the Bitcoin network.



**Collateral function**

As the core collateral of bitcoin derivatives and trusts, it is the Risk Modeling standard of bitcoin finance and the main tool to improve trust creditworthiness.



**Metrics**

The measurement standard in POS consensus elections . The more votes people get, the greater the responsibility. It is also a mortgage and voting tool for on-chain governance.



**Market value unit**

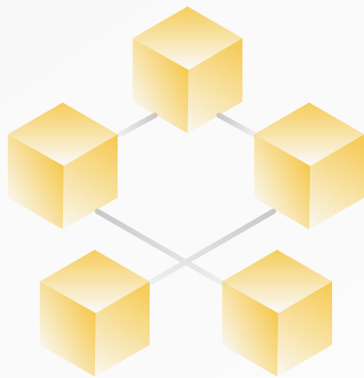
As the unit for asset mining, all assets are converted into votes based on the PCX price, similar to ECR20 in Ethereum.



**Exchange medium**

In the system-integrated transaction Dapp, it serves as the base currency and exchange medium for obtaining other assets.

**Tricameral governance structure is adopted by ChainX at the advice of Polkadot for better decentralized community governance, including Referendum Chamber, Council and Technical Committee. In addition to the three, X-Association and Treasury are introduced to enrich the framework of community autonomy.**



## Referendum chamber

The Referendum Chamber has the most members (all token holders) and the highest authority. All "legislations" (Runtime logic modifications) must go through a democratic referendum. Now that ChainX is based on Substrate2.0, the community or Council can submit a proposal for referendum. If approved, the system automatically modifies ChainX's Runtime logic and upgrades without forking.

## Council

Given the fact that referendum alone cannot rule effectively, that's where the Council comes handy in dealing with day-to-day affairs. Council members are elected by token holders with Phragmén election algorithm. There are currently 11 members on the Council and 7 more as alternates, with re-election every 24 hours which generally sees few changes.

### Council election

Participation	Users who run for the election should submit a candidate application form to the Council with 10 PCX staked which will be returned if they are elected as a member or alternate, otherwise the Treasury will lay claim to it. This mechanism helps eliminate malicious participation which unnecessarily occupies chain resources.
Voting	Users holding PCX can cast their ballots at the Council page. Each vote at most selects 16 candidates with the amount of voting assets specified and 0.01 PCX staked. Casted votes can be withdrawn at any time with staked assets returned.
Announcing result	Each election cycle lasts one day. Votes are counted after the cycle to form new Council.

**Main responsibilities of the Council**

---

**Revoking penalties**

The Council has the right to revoke staking penalties caused by network errors if the threshold of at least 1/2 of the members is met.

---

**Submitting referendum proposals**

The Council has the right to submit a referendum proposal to upgrade the RUNTIME logic if certain consensus is reached within the Council.

---

**Calling out a referendum**

The Council has the right to call out a referendum at the last minute with 2/3 majority when a malicious or wrong referendum proposal is about to implement. Staked assets behind the improper proposal are confiscated by Treasury.

---

**Voting on Treasury proposals**

The Council votes on Treasury proposals and Tips which are approved if 3/5 or more members agree, and rejected if over 1/2 members disagree.

---



# Technical Committee

Technical committee is made up of the technical team of ChainX network with PolkaX development team currently serving at the committee. The committee reinforces and counterbalances the Council, and vice versa, forming checks and balances.

## Main responsibilities of the technical committee

---

### Submitting emergency proposals

Technical committee has the right to submit an emergency proposal with the Council’s permission when a bug or upgrading need is detected. The proposal immediately goes through the referendum without further delay.

---

### Vetoing the Council’s referendum proposals

Technical committee has the right to veto proposals with the Treasury getting the staked assets if unanimous agreement is reached within the committee or the root cause (such as sudo or Council) triggers the process.

---

# X - Association

X-Association, a non-profit organization, is fully committed to the development of the chain of ChainX and surrounding ecosystem. X-Association is composed of experts and enthusiasts who are no stranger to ChainX’s chain, community management, blockchain technology and development, and stand ready to contribute to ChainX for a long time.

## X-Association membership

The initial members including 1 secretary general and 4 secretaries are elected by the Council, but to ensure management efficiency and continuity, X-Association when fully established, decides the replacement of personnel on its own and reports to the Council about the changes. The council has the right to remove one or more members with two-thirds majority. Dynamic working groups under X-Association, led by the secretary general or a secretary, are set to complete specific tasks.

### With the permission of the Council, X-Association performs the following duties

Providing advice or consulting services to the development and new planning of the chain

Supporting, promoting and governing ChainX communities (fans and developers)

Providing direct technical support to ChainX’s users and developers

Coordinating and managing various development teams of the chain

Releasing reports on work and fund usage on a regular basis to the council and the community

## X-Association’s funding source and funding management

X-Association has a separate PCX account to which grants from the Council are issued regularly. The account is a 3/5 multi-signature account with the secretary-general and 4 secretaries holding private keys respectively. The account is renewed if there are personnel changes.

# Treasury

The Treasury is a PCX funding pool to which staking penalties on the network, residual income of inter-chain mining, staked assets in running for the Council election, and confiscated assets of failed proposals flow. The Treasury provides financial support to projects promoting ChainX development and facilitating ecosystem growth. As the network grows, contributing individuals, organizations and companies are eligible to apply for treasury funds as incentives.

**Contributions Include but not limited to the following areas**

Infrastructure deployment, usage and maintenance	Network security, such as monitoring services, auditing, etc
Ecosystem support, such as cooperation with third-party blockchains	Marketing activities, including advertising, cooperation, etc
Community activities and PR events, such as meetups, ChainX parties, etc.	Software development, such as wallet, client development, etc

# Bitcoin financial platform

Bitcoin, with its market value reaching 470 billion U.S. dollars, holds the key to the digital currency world and leads towards deeper blockchain breakthroughs, which indicates that Bitcoin is being re-recognized as a payment method, perhaps only a tip of the iceberg in terms of its full potential. ChainX committed to the research on the expansion of Bitcoin's Layer2 financial platform strives to promote Bitcoin's value flow, enrich its financial derivatives and improve the hedging tools.

## Bitcoin trusteeship

The Bitcoin network cannot integrate light nodes of other chains to form smart contracts, which means assets are trapped in their own systems. ChainX came up with a scheme to break the dilemma with the "light node + trusteeship" scheme that allows chain crossing. So far Bitcoin light-node bridge and X-BTC1.0 trusteeship scheme have been finished, enabling completely decentralized mapping of Bitcoin onto ChainX. In addition, the latest logic framework of X-BTC trusteeship has been established and will be launched in the foreseeable future.

### X-BTC1.0—Trust node trusteeship scheme

In X-BTC 1.0, trustees are good-performing nodes in ChainX's testnet, with new nodes chosen by abdicating ones, which requires the Council's permission before taking effect. There is a hot multi-signature address or contract and a cold one generated by each trust node. Funds are transferred to new addresses after each renewal with users having access to the real-time data of inter-chain assets flow and reserves, thus no trust node can unilaterally misappropriate the fund.

In X-BTC 1.0 trusteeship scheme, users initiate a transaction from a Bitcoin account to a multi-signature trustee address by adding ChainX's account address in the Note to bind the two addresses together, which once done, does not need repeating second time for the network can automatically recognize the binding. X-BTC is issued based on the transactions of users' Bitcoin address.

X-BTC 1.0 trusteeship process

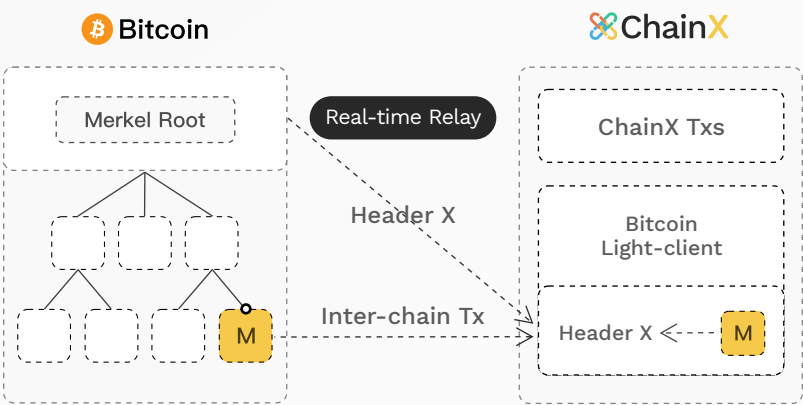
Inter-chain deposits

Run Bitcoin light nodes on the chain, and send Header in real time by Relay to keep the longest chain updated;

Users transfer assets to the hot address of a trustee with ChainX address in hexadecimal form and other information attached to OP\_RETURN with which transfer bridge can identify related ChainX users;

Relay monitors the Bitcoin network and submits related information including Tx Proof path and OP\_RETURN to the transfer bridge after pinpointing the block in which this transaction is located and obtaining the permission from the chain.;

The transfer bridge after verifying Tx and OP\_RETURN note decrypts the ChainX address attached to OP\_RETURN and issues the transferred amount to that address.



Inter-chain withdrawal

Users submit a Bitcoin withdrawal application to ChainX;

The recording module in ChainX transfer bridge or gateway locks the corresponding X-BTC and keeps the application information in record which is trackable with a unique ID;

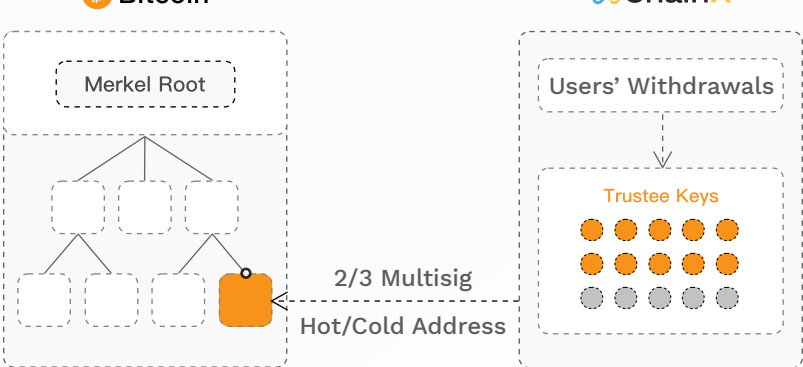
The withdrawal information is periodically obtained by a trustee which forms the withdrawal text;

ChainX transfer bridge locks the corresponding withdrawal amount after receiving the text which also requires other trustees to sign;

Relay submits the text after required signatures are signed to the Bitcoin network;

Relay then submits the withdrawal transaction and its proof path to the transfer bridge after the transaction is confirmed;

Transfer bridge closes the withdrawal record and destroys the locked X-BTC after Tx id proved to be valid.



X-BTC2.0—Vault trusteeship scheme

X-BTC 2.0 is a trustless and highly efficient inter-chain asset system based on the XCLAIM framework through which two protocols are introduced to enable distributive, transparent, consistent, and anti-censorship cross-region blockchain transactions. The most prominent difference from X-BTC 1.0 is the Vault (asset custodian) mechanism which allows more people to engage in assets' chain crossing.

X-BTC 2.0 Vault advantages

XCLAIM overcomes the limitations of centralization in the following ways

Security auditing log

Build a log to record all users' behavior on Bitcoin and ChainX

Proof of transaction inclusion

Relay is used to prove to ChainX the correct behavior on Bitcoin

Proof or punishment

XCLAIM does not rely on last-minute fraud proof (which renders the system passive), but requires proactive proof of correct behavior

Excessive collateral

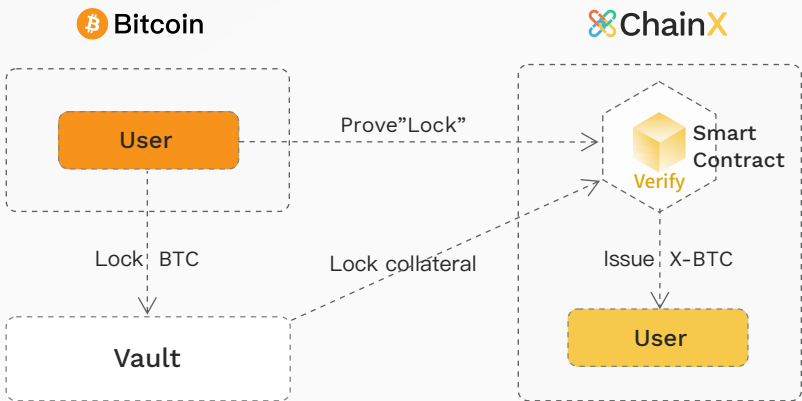
Untrusted Vaults, subjected to collateral (PCX), have to establish a mechanism to mitigate exchange rate fluctuations



X-BTC 2.0 Vault scheme process

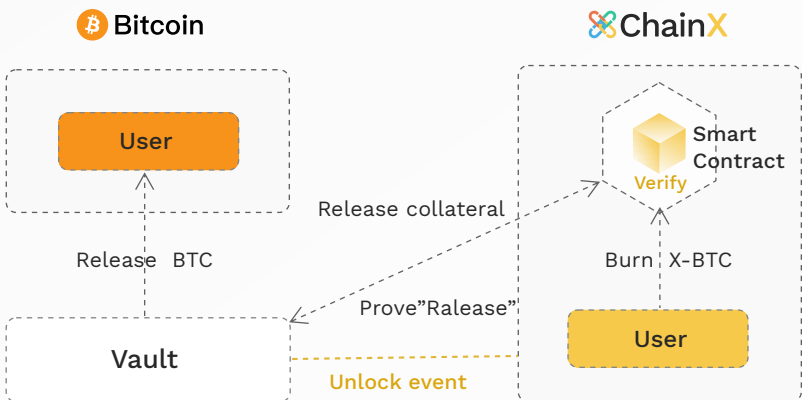
Inter-chain deposit

- Vault locks collateral on the ChainX chain;
- Users transfer Bitcoins to Vault for locking;
- Submit lock proof to ChainX;
- ChainX smart contract locks the amount in Vault and issues X-BTC to the user's account.



Inter-chain withdrawal

- Users burn X-BTC through ChainX smart contract;
- Vault transfers Bitcoins to the user after witnessing the unlock event;
- Vault submits the release proof to ChainX to unlock the collateral.

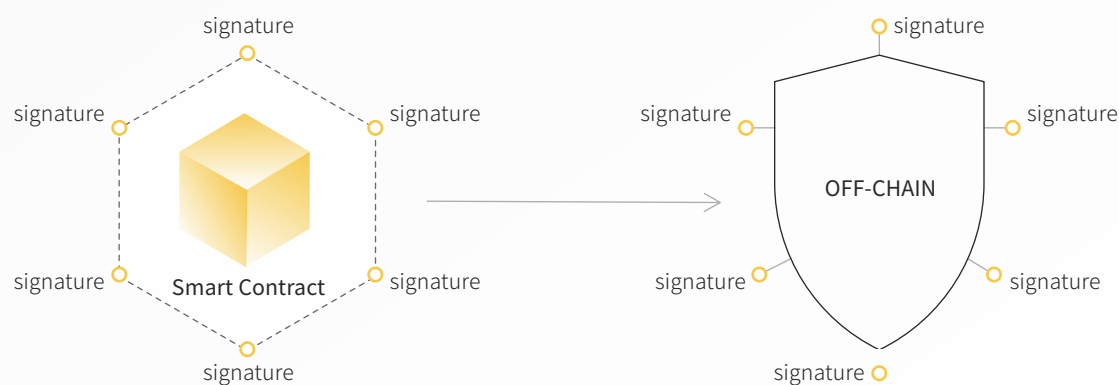


X-BTC 3.0—MPC-based  
trusteeship scheme

X-BTC 3.0 manages to cross assets onto other chains with MPC in a network composed of Trader nodes which contribute computing power to sustain the system. There are two main branches in MPC (Multi-party Computation): "secure multi-party computation based on garbled circuits" and "secure multi-party computation based on secret sharing", and X-BTC 3.0 uses the latter which is based on Shamir's Secret Sharing to encrypt and send out data.

ChainX plans to start with 100 seats and 28-day election cycle. All trader nodes are randomly grouped with the private key pieces they are holding renewed every 48 hours. Assume each group has N nodes, and each transaction requires signatures of at least M nodes( $M < N$ ) to be approved. There is also a punishment system in place to deter trader nodes from violating the agreement for improper gains.

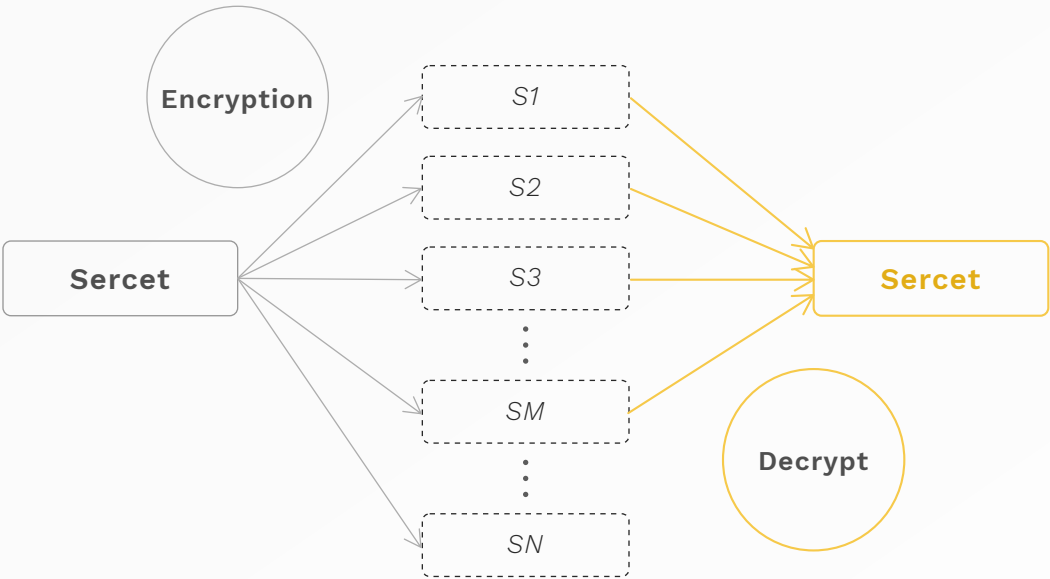
The main advantage of X-BTC 3.0 is the complete decoupling between MPC and the contract module, which means the chain is able to connect with other chains as long as the MPC algorithm is supported by the chain and compatible with other chains. MPC's high compatibility with multi-chain system is a prominent advantage and it is off-chain, which avoids the risk of contract being hacked, another highlight.



How MPC works

Assume there are N participants. One of them divides a private key, a password or sensitive information into N encrypted pieces and sets the retrieve threshold at M ( $M < N$ ). This type of encryption and decryption is usually referred to as multi-signature. For example, 3/5 multi-signature requires at least 3 parties' signature (encrypted pieces in Shamir's Secret Sharing) to enable transactions (decrypting the original private key, password or sensitive information).

The private key pieces are held by trader nodes who need to cooperate with one other to complete a transaction. Users can become trader nodes by collateralizing assets, and contribute their computing power for financial gains without their identities being revealed.



## **X-BTC 4.0—Decentralized and autonomous trusteeship scheme**

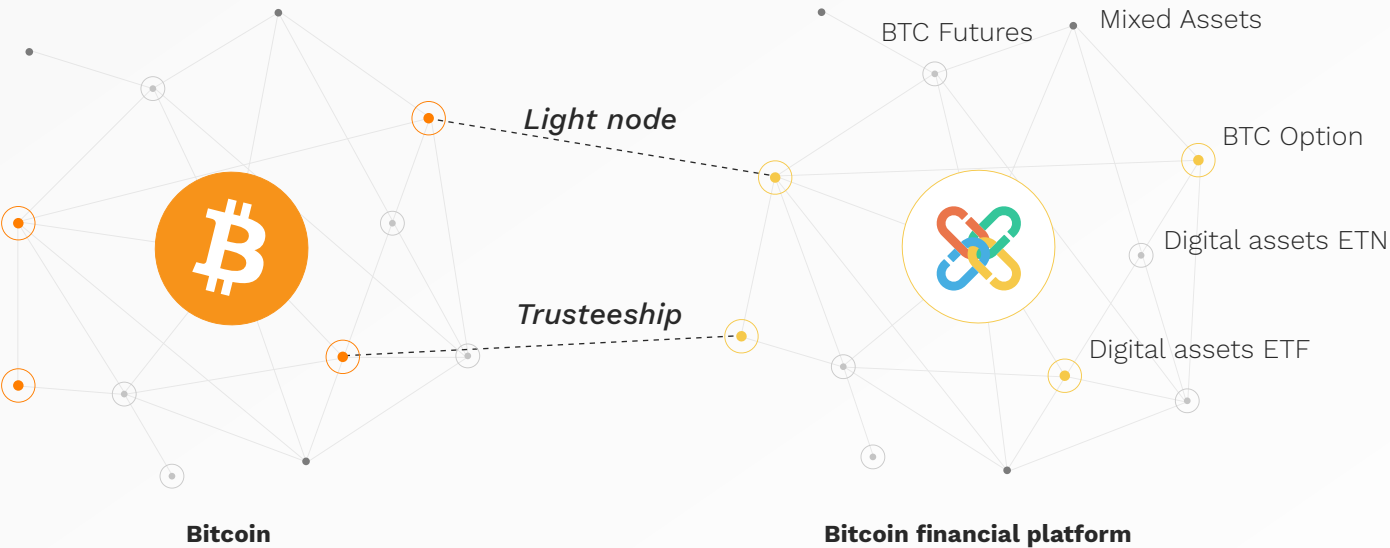
X-BTC 4.0 modifies the MPC algorithm and resets the threshold to enable users to hold the private key pieces themselves, what's more the pieces they hold have the veto right, which means a user's assets cannot be moved without his or her involvement in decryption, thereby guarantees BTC asset security in the trust and greatly reduces the amount of collateral needed to a level even lower than the amount of inter-chain assets. This is the most ideal solution.

**For example, if a user wants to redeem X-BTC, the steps are as following**

- Calculate the number of needed encrypted pieces and send the request to relevant trader nodes;
- N trader nodes respond with their own pieces;
- These nodes then send the request to other trader nodes in the same group;
- When a node receives more than M pieces, Signature\_share\_nodes are constructed, along with Signature\_share\_user to retrieve the private key and complete the transaction signature.

# Bitcoin derivative platform

With record market value and decreasing fluctuations, Bitcoin is recognized by more mainstream institutions and has gradually become a store of value. Against this backdrop, there are growing demands for hedging and leveraging tools when it comes to digital asset investment. To meet the demand, ChainX aspires to become the biggest Bitcoin layer 2 financial platform with derivatives like Bitcoin futures, options, synthetic assets and swap agreements.

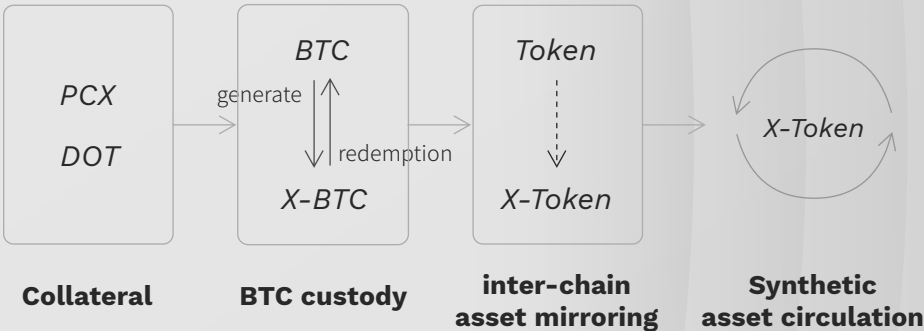


# Digital asset gateway

ChainX asset gateway is composed of two parts: decentralized Bitcoin trusteeship and inter-chain asset mirroring. Users deposit and collateralize bitcoins for X-BTC which is used in transactions with synthetic assets of other cryptocurrencies, so that all sorts of cryptos can be exchanged and traded on the same chain.

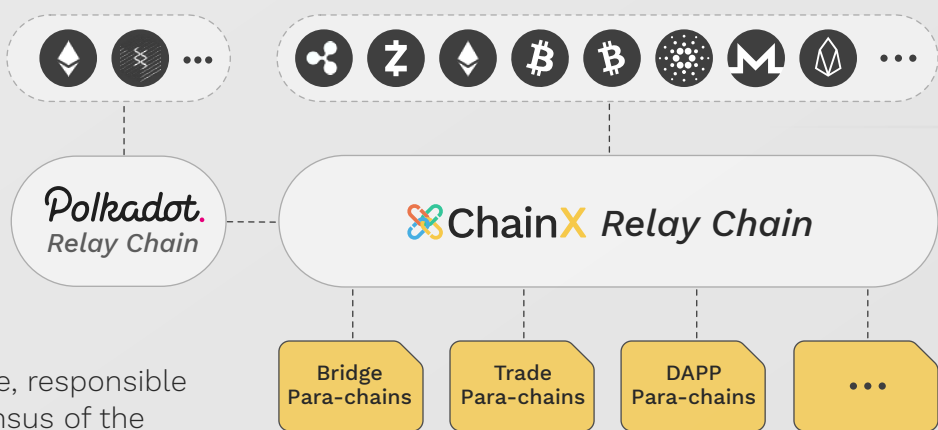
Synthetic asset of cryptos is a mirroring simulation of the target asset. Like derivatives in the traditional financial market, virtual assets pegged to cryptocurrencies are created, with blockchain functioning as the traditional trading market. In short, what the synthetic asset does is to copy prices of original cryptocurrencies, so that people can directly trade these virtual assets on the chain.

ChainX inter-chain asset mirroring uses X-BTC as locked collateral to map or generate synthetic assets which can be exchanged through smart contracts without requiring a trading medium. ChainX rewards X-BTC holders who issue synthetic assets for the contribution they've made, thereby encouraging users to hold and lock X-BTC whose value is pegged to Bitcoin.



# Polkadot second-layer relay chain

Parachains are developed using different types of blockchain technology, and relay chains are responsible for safeguarding the network’s co-sharing consensus and facilitating inter-chain transactions among parachains. Relay chain itself does not deploy any applications. It is parachains that develop and deploy applications. Polkadot focusing on efficient inter-chain connection within its ecosystem advances the entire blockchain development to a new level and looks set to usher in blockchain 3.0. ChainX will run as the second-layer network to Polkadot after it releases the 2.0 version.



## ChainX relay chain

The highest security guarantee, responsible for the overall security consensus of the second-layer network.

## Parallel transfer bridge

Split transfer bridges to independent parachains to share the burden.

## Transaction parachain

Provide free matching services to assets within the system to improve transaction throughput.

## DAPP Parachain

Various applications developed by the community can run independently with inter-chain connection being in place.







<https://chainx.org>