TBD [redacted]

System White Paper
2019.09.10

Beidou block chain

High Extensible Public Blockchain Networks for Practical Applications

Beidou Block Chain Foundation/Consensus Alliance

Fast Access Blockchain Foundation

Directory

1. overview

Block chain technology is the foundation of the next generation Internet - value Internet. The successful operation of block chain platforms such as Bitcoin and Ethernet Square has shown good prospects for block chain applications.

However, due to the constraints of communication, node performance and consensus mechanism, the current public block chain system is faced with the bottleneck problem of seriously insufficient transaction processing capacity, such as Bitcoin processing volume is not more than 7 per second.

this is a huge obstacle to block chain moving towards practicality. in real economic activities, trading volume exceeds this scale in many application scenarios, such as exchanges, iot platforms, e-commerce platforms, supply chains, medical care, etc. the actual trading volume of a single platform tends to be tens, hundreds, or even thousands per second. while the public block chain is simultaneously oriented to many application scenarios, the actual processing capacity is much higher.

It is urgent to solve this problem.

Beidou enterprise system company block chain research and development team, three years of in-depth exploration and research, put forward a number of breakthrough innovative technologies, launched a new block chain system architecture with good expansion performance perfect design scheme-fast public block chain (Beidou chain) system (The Big Dipper - TBD), committed to effectively break through the block chain technology barriers, paving the way for the construction of block chain systems to meet the needs of practical commercial applications.

Beidou public block chain system (The Big Dipper), also known as Beidou chain (TBD), is composed of three parts of integrated design-basic block chain, auxiliary block chain and open storage architecture. It is a trinity and cooperation. It has a unified protocol foundation, coordinated functions, full process legitimacy and validity verification, truly decentralized, safe and reliable high performance block chain complete architecture.

1.1 Systems Design Principles and Philosophy

Beidou chain strict design logic is based on strict design principles and philosophy, the distinct characteristics of block chain system conflict with application requirements, technical methods and practical conditions are contradictory, difficult to reconcile, system design needs to follow the principle of complete causal cycle, which is based on a set of philosophical ideas.

1.1.1 System design principles

Build trust – this is the core mission of the blockchain, and the system is designed to build a trusted system for applications.

Decentralization – is the core feature of the block chain and the fundamental means of constructing trust.

Open Architecture - Openness is essential for decentralization. Openness means equality for all, open source of code, and civilianization of facilities.

Application Oriented - Open architecture leads to equal participation, equal use, and non-trusted participants need assurance of trust mechanisms.

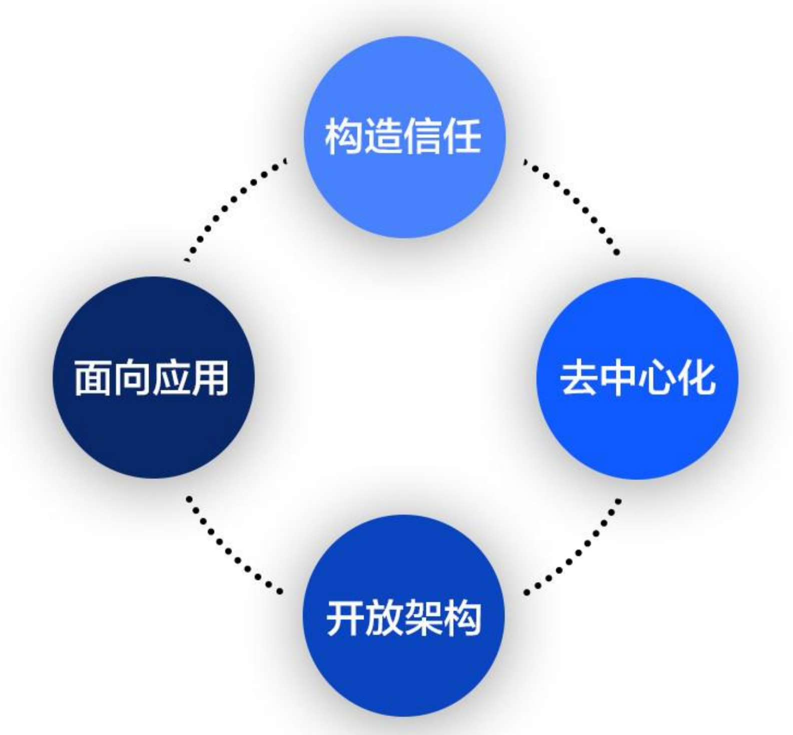


Figure 1. System design principle diagram

1.1.2 Philosophical thought

Building the system according to the above design principles faces an irreconcilable contradiction: decentralization, scalability and reliability can not be combined, decentralization and expansion, the system is unreliable; extensible and reliable can not be decentralized; decentralization and reliability can not be extended.

To solve this contradiction, we need a set of feasible philosophical theories, and we conclude four philosophical principles:

Trust comes from non-trust-block chain system is trustworthy, but the participating nodes do not trust each other.

but local nodes

The centralization and decentralization of non-voting power - extending local nodes to form centralization, if the decision is turned into decentralization;

Reliable unreliability - decentralized local central nodes are unreliable, but decentralized adjudication mechanisms are reliable.

1.2 Technical elements

According to the system design principle, focusing on the core characteristics of the public block chain while facing practical commercial applications, we must solve the philosophical contradiction, which requires not only theoretical solutions, but also feasible technical methods.

1.2.1 Measures to relieve theoretical contradictions

In order to eliminate these objective contradictions, we need innovative thinking, we put forward a new solution: to construct and restrict the dislocation structure.

The restriction of each link of the system is connected with the carrier organically, but the restriction of each link of the system and the wrong position of the carrier can effectively solve this problem. To this end, the following design ideas were established:

build an open public blockchain-basic blockchain, which is highly decentralized but difficult to extend, and must target minimum amount of data, minimum amount of computation, minimum network bandwidth to achieve maximum openness, maximum decentralization, and maximum reliability. such a system is not scalable, but applications require systems to be extended.

Build the auxiliary chain, from the local implementation of expansion-the practical application requires the system to have a strong processing ability, so it is necessary to make the system have scalability, the extension dislocation into the local node, become a feasible way, but such a system presents centralization, become distrustful.

Establishing an open storage system to decentralize data and decisions, the local node's off-chain and centralization features make it untrustworthy, it is necessary to de-centralize the mechanism, thus establishing a decentralized open storage architecture, but the storage architecture can not form a complete decentralization mechanism, so the design SCAR mechanism is associated with the decentralized underlying block chain.

1.2.2 Technical measures achieved

In order to realize the integrity of dislocation mechanism, only basic chain, auxiliary chain and storage mechanism are not enough, and other technical means are needed.

For this reason, we put forward three key technology application schemes: KanBan、SCAR、Sharding the technical scheme which is matched with the basic chain, the auxiliary chain and the storage system respectively.

Among them, Sharding refers to the technology in existing big data, which is used as fast data query and consensus decision.

KanBan and SCAR are our innovative designs in the block chain system;

The basic block chain +KanBan - auxiliary chain +KanBan - SCAR - the contradictory dislocation architecture supported by open storage architecture +KanBan - MapReduce technology form a complete solution.

The composition and interrelationship of technical measures are as follows:

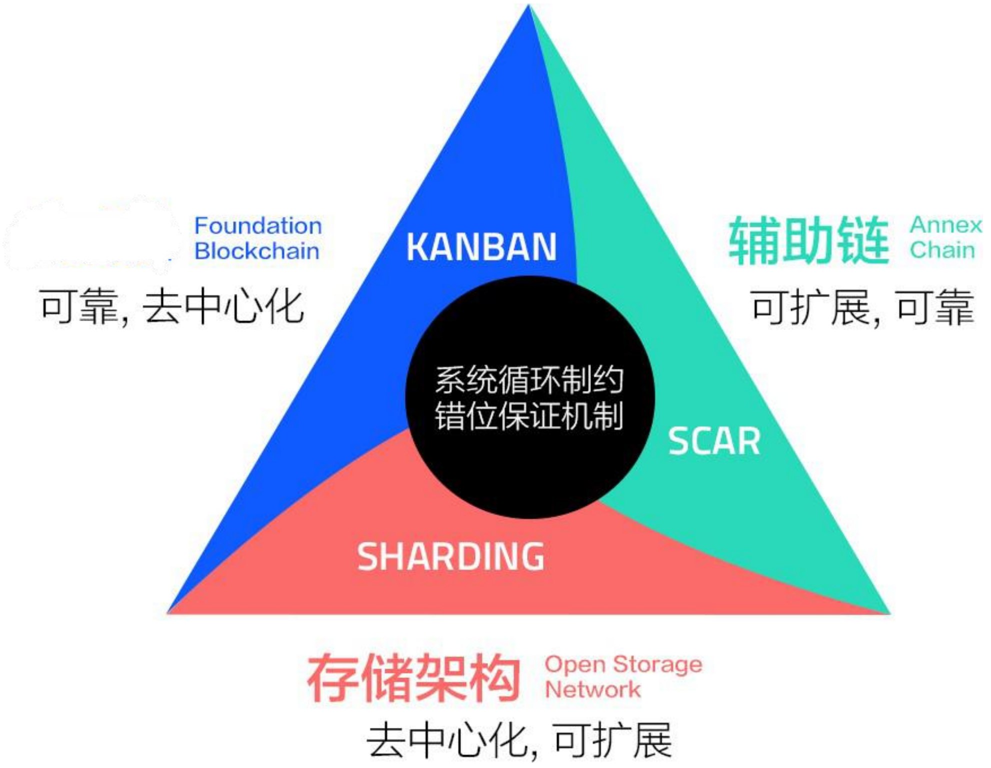


Figure 2. System circulation restriction dislocation guarantee mechanism

In order to streamline the program and make it easy to implement, and to make the system more broadly adaptable to standards, we propose three innovative technology protocols:

Cross-chain unified address agreement (CCUA - Cross

Chain Unified Address); transaction swap agreement

(TEP - Transaction Exchange Protocol);

An open verification rule protocol (OVP - Open Verification Protocol);

At this point, the system in theory and technology has a complete solution, but also widely compatible with the preparation conditions.

These measures provide adequate theoretical and technical guarantees for decentralization, trustworthiness and scalability of the system as a whole, and provide for such precautions

It provides a practical and effective means for the system to break through the bottleneck of blockchain technology, and successfully solves the problems of decentralization, security and scalability in the development of blockchain.

this system is the first public blockchain system that truly meets the needs of practical commercial applications.

2. Technology Programme

Because of the different communication conditions and node processing capacity and the constraints of consensus mechanism, it has become a recognized fact that the bottom layer of the public chain can not handle a large number of transactions alone, so to break through this obstacle, we must innovate in the overall architecture.

2.1 System architecture

The fast block chain system aims to use the benefit incentive mechanism to construct a fast, low-cost, efficient, safe and reliable decentralized public block chain economic ecosystem to meet the large-scale daily business needs.

The system consists of three parts: the basic block chain (Foundation blockchain), the auxiliary chain (Annex chain) and the open storage architecture (Open Storage Architecture), which are the components of the open economy ecology based on the contradictory dislocation mechanism and the core rules of the consensus mechanism.

The overall logical architecture of the system is shown below:

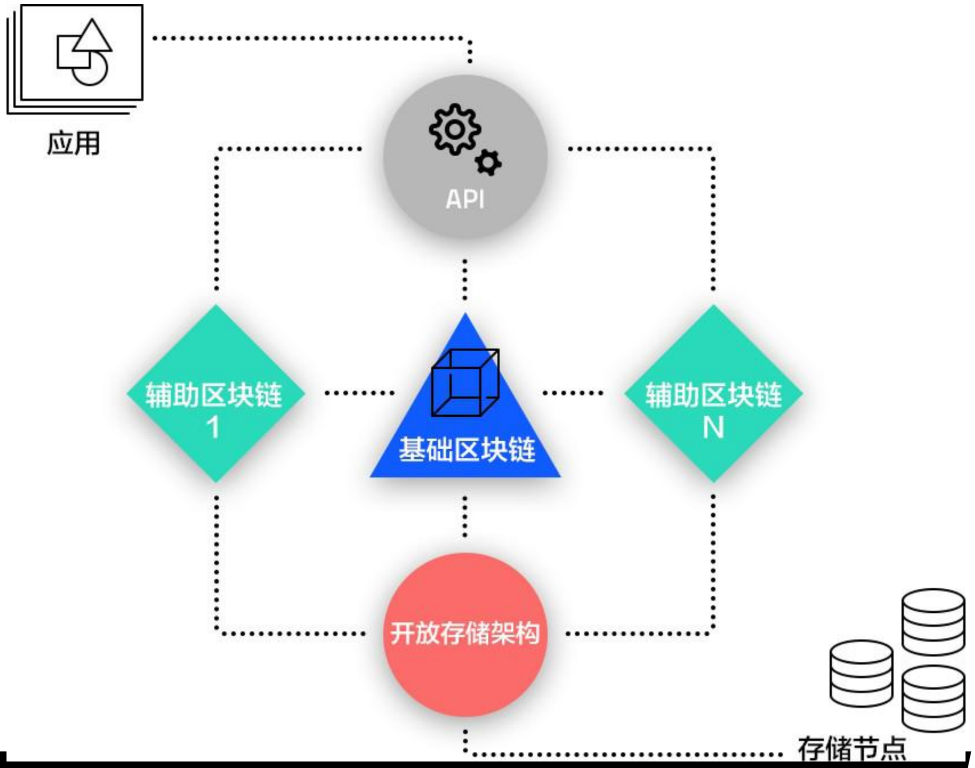


Figure 3. General logical architecture of the system

Unlike the existing main chain/side chain mechanism of bitcoin, the basic chain-assist chain-storage architecture is a complete architecture designed by the underlying protocol. The data encryption and verification mechanisms are compatible and cooperate with each other.

The design idea of the system is: the basic block chain aims at the minimum amount of data, the minimum amount of calculation and the minimum network bandwidth requirement, providing the underlying protocol, the intelligent contract, the ultimate account book, the ultimate adjudication right; the auxiliary chain or regional node performs large-scale local off-chain transactions; and the open storage architecture ensures the decentralized storage of local data.

The system proposes three technologies, KanBan、SCAR and CCUA, so that the local off-chain trading state can be updated and verified in real time in a decentralized manner throughout the block chain, so as to prevent double flower, so that the system can meet the requirements of centralized large-scale real-time trading, including large trading volume scenarios such as exchanges, Internet of things, e-commerce, supply chain, medical treatment, etc. To enhance the decentralization function of local transactions, the system designs an open storage architecture support decentralized open storage of local transactions through agreements and consensus mechanisms with economic incentives and mandatory rules.

The incentive mechanism of the base block chain is mining income, the incentive mechanism of the auxiliary chain is business income and mining income, and the incentive mechanism of the storage node is data, cost and mining income.

2.2 Base Block Chain (also known as Main Chain)

The basic block chain is the core of the system. The design aims at the minimum amount of data, the minimum amount of calculation and the minimum network bandwidth requirement. It mainly provides the basic protocol, account book, intelligent contract, value system, and has the highest adjudication power. The trust legitimacy of the basic block chain comes from all participating nodes.

the underlying blockchain design uses a Proof-of-Production (pp) consensus mechanism combined with production, a hybrid mechanism of proof of equity and proof of productivity, but still uses a PoW consensus mechanism similar to bitcoin before it has sufficient productivity.

2.2.1 The function of the whole node of the base block chain

Base block chain full node in addition to the usual block chain, wallet, miner, routing, virtual machine and other functional modules, especially the introduction of KanBan functions. KanBan means "Kanban" in Chinese, derived from the modern supply chain / manufacturing chain system, where workers are engaged in fixed process work, but KanBan provide instant information to everyone to prompt attention or special changes.

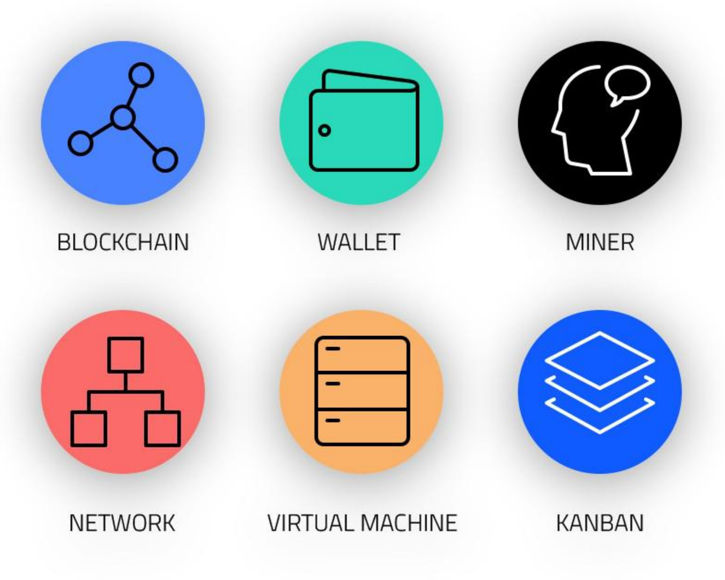


Figure 4. Whole-Node Function Composition of Base Block Chain

2.2.2 KanBan

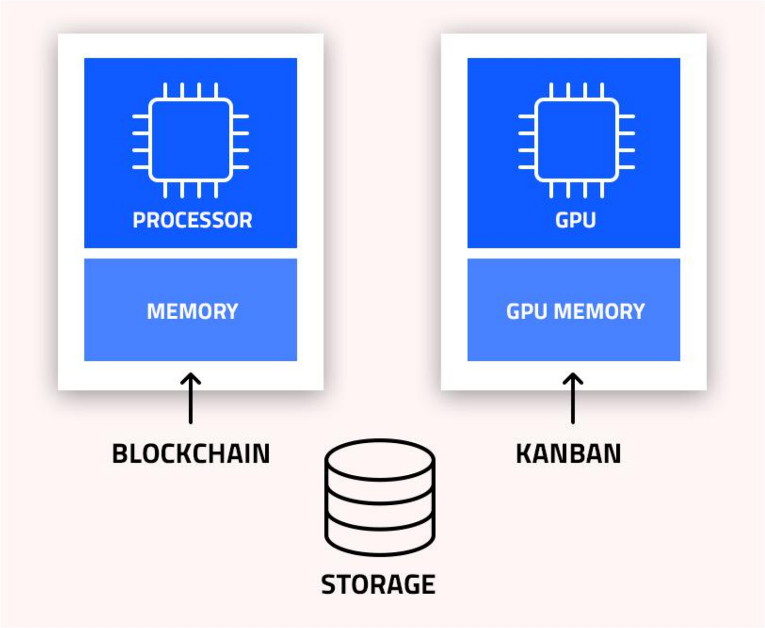


Figure 5. Schematic diagram KanBan base block chain nodes

KanBan is designed to provide real-time update and query ability to the transaction status of the auxiliary chain in the global scope without significantly increasing the burden of the main block chain, which is a special module designed to effectively prevent the double flower attack of the auxiliary chain.

This system KanBan designed as GPU memory database. On the one hand, it does not occupy common resources of nodes and ensures the efficiency of basic block chain operation. On the other hand, GPU memory database data processing ability far exceeds that of the main computer processor, which can greatly improve KanBan operation efficiency. Make small batch status update and query operation can be completed in milliseconds.

Because of the KanBan function, the transaction of auxiliary chain is presented globally in real time in a decentralized way, which can effectively realize the purpose of preventing double flower. since the KanBan runs in the GPU of the computer and takes up GPU memory, however, for nodes running GPU based miner software, miner software shall be run separately from the KanBan in a different computer.

The maintenance and update of KanBan state is controlled by intelligent contract, and there is a strict validity verification and confirmation relationship between KanBan and main and auxiliary chain nodes and storage nodes to ensure the accuracy and legality of KanBan data.

The KanBan process is to receive packages from the auxiliary chain → verify the legitimacy of the package → verify the legitimacy of the transaction → update the status of the KanBan. → submit receipt to auxiliary chain.

At the end of this KanBan, the exact status of the address or account in the secondary chain transaction is kept, and the detailed transaction records on the secondary chain can be further verified to the storage node if necessary.

2.2.3 Data in KanBan

Auxiliary List:

Number	Public key	**Hash of the last block**	**Merkle Root of unlocked block transactions**	Public key	Public key
1	ds5kgce3…vd34	ew98gweio309	hgurs2ua6serhufdsfe423	40000	20160223T021405
2	ly8r5gdt4s…gte	rc6ghd8fjcndu9	goir7q3c9sk4ge8rd3afrb	1200000	20160508T223611
…	…	…			…
n					

Figure 6. Auxiliary linked lists in the KanBan

Address (Account) Status Table:

Address	Balance	Suspicious	Time

m5frtfgdesr……0	200000	F	20160312T100325
msetvuehfe……0	16000000	T	20160520T081220
…	…		…

Figure 7. Address status table in KanBan

Unlocked Block Transaction Table:

Transaction Number	Address	Address	Quantity	Time
1	ds5kgce3…vd34	ew98gweio309	40000	20160223T021405
2	ly8r5gdt4s…gte	rc6ghd8fjcndu9	1200000	20160508T223611
…	…	…		…
n				

Figure 8. Table of Unlocked Block Transactions in the KanBan

KanBan verify the validity of the package and its transactions after receiving the auxiliary chain packet, update the relevant address status after verification, and return the receipt to the auxiliary chain and notify the storage node, including node balance, contract signature, reject if not qualified and notify the auxiliary chain.

KanBan can provide the current status of each address in real time to prevent double flowers. KanBan also provide the signature stub of the current block of each auxiliary chain to confirm the validity of the block in the auxiliary chain.

2.2.4 Validation of transaction validity

For the new transaction on the auxiliary chain, the system verifies the validity of the transaction through the KanBan state and the underlying block chain transaction state. For the same account or address conflict, time priority, the same time, hash value priority.

If a transaction conflicts, a suspicious identifier is set for the address or account that causes the conflict.

For addresses with suspicious tags in KanBan, detailed transaction records are checked through the open storage architecture node when a new transaction occurs.

technically, in order to enhance the performance of KanBan processing, a special GPU data processing module is developed to make the KanBan run in the node computer GPU without occupying the common resources of the node, so that it can effectively handle the underlying block chain transactions.

KanBan in addition to the rapid processing of auxiliary chain transactions,

maintenance of auxiliary chain address status, but also perform auxiliary chain

mining task. KanBan can also periodically mirror data to the hard disk for

rapid recovery after power off.

2.2.5 Composition of KanBan in basic blockchain network

KanBan can run in the base block chain node master computer, or in the independent master computer associated with the base block chain node, or even in the storage node master computer. Technically, a node can also have no main chain node, auxiliary chain node or storage node, but just a separate KanBan node.

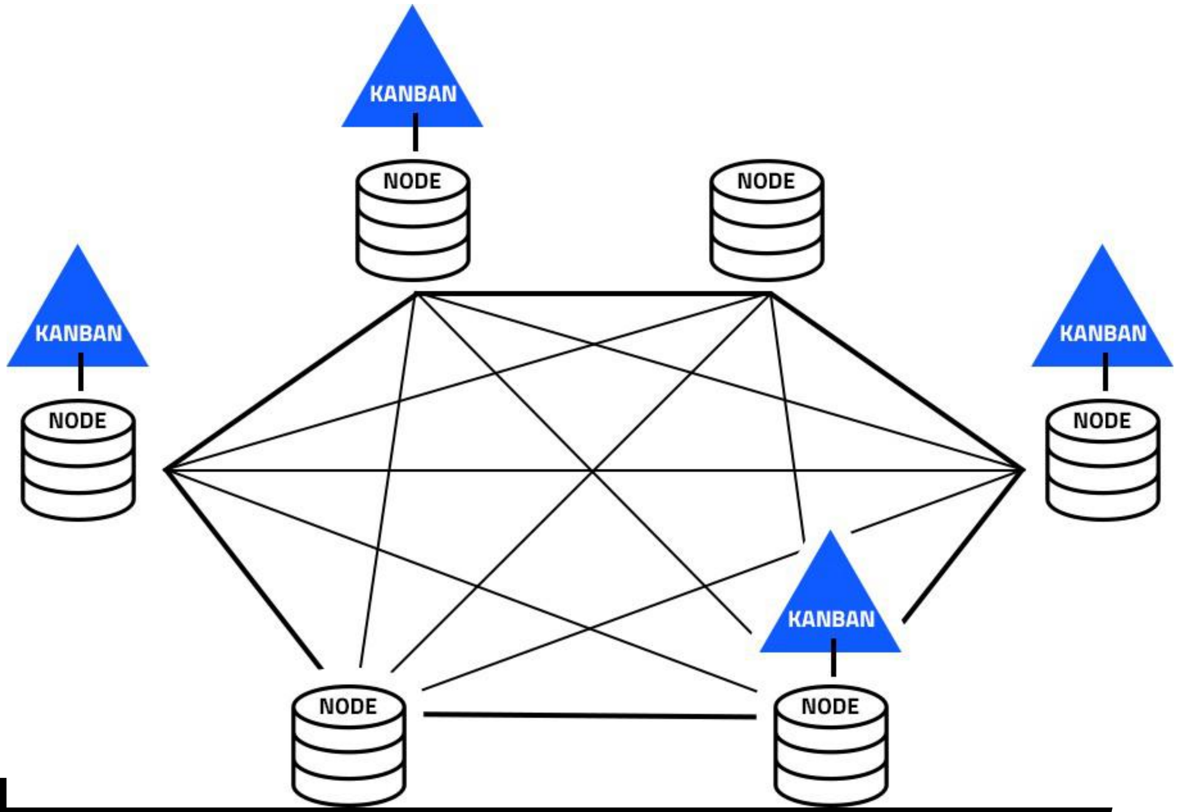
Since KanBan program is designed as a GPU database program that runs in computer GPU and takes up GPU memory, devices that do not have appropriate graphics acceleration cards can not run KanBan..

the design scheme, the system does not require all full nodes on the base blockchain to have KanBan functions, but the nodes with KanBan functions have KanBan identification.

nodes without KanBan functions do not participate in KanBan services or in the co-chain consensus mechanism; nodes providing KanBan functions can earn the co-chain mining proceeds, which come from the transaction costs of the co-chain.

Actually, for nodes with better basic conditions, all system functions including basic block chain, KanBan、 auxiliary chain and open storage node can be provided.

A schematic diagram of the underlying blockchain network and KanBan distribution is as



follows:

Figure 9. Main block chain network diagram
(not all nodes are KanBan nodes)

2.2.6 KanBan configuration requirements

to run KanBan, node computer must be equipped with a graphics acceleration card to run the appropriate algorithm. the hardware requirement of the initial KanBan node is to install a graphics acceleration card with more than 16 GB of memory, but the requirement will increase as the amount of data increases.

improving GPU hardware requirements does not affect consensus mechanisms, but may affect operational effects. Since KanBan nodes in the system are classified according to performance and are identified separately, such as 16 GB as KB2..

Suppose that 2 GB GPU of memory is reserved for other purposes of the node ,2 GB is used as auxiliary chain related data, and the rest is used as the most important off-chain account address status table.

One account status record data does not exceed 64 bytes ,12 GB can provide about 200 million active account status records; if 32 GB graphics acceleration cards are installed, about 500 million active account status information can be provided.

System design, support KanBan grouping function, a set of KanBan to serve a certain or some auxiliary chain.

2.2.7 Basic blockchain implementation plan

The core of the improved implementation of the basic block chain is to increase the support for KanBan、SCAR and CCUA, increase the auxiliary chain verification and root contract state setting mechanism, increase the intelligent contract mechanism, and reduce the amount of transaction and block data.

The core architecture is shown below:

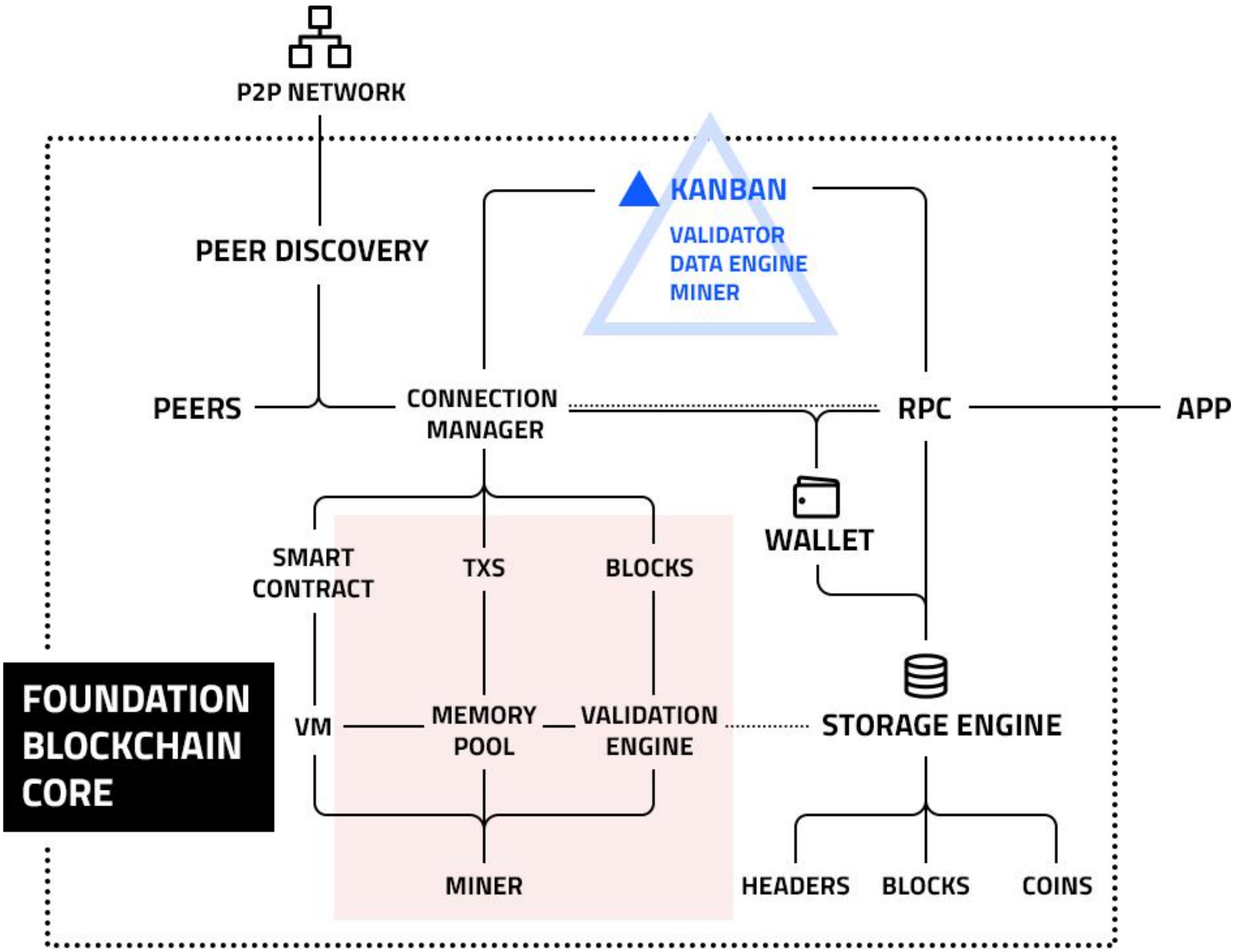


Figure 10. Basic blockchain kernel architecture

The system development adopts streamlined independent module structure, which is easy to configure, manage and maintain. Many modules in the kernel of the base block chain will also be used in the auxiliary chain and open storage architecture module.

2.3 Auxiliary chain

Auxiliary chain is an important part of the system, usually auxiliary chain nodes carry a large number of specific business, such as exchange transactions, e-commerce, supply chain, Internet of things platform or medical platform.

According to the design of the system, the value confirmation and the final decision of the transaction are carried out in a decentralized manner by the base chain, and the decentralized data storage of the open storage architecture is combined.

According to the system design, even if an auxiliary chain is designed for fraudulent purposes, it can not cause any loss to the off-chain customer.

2.3.1 Auxiliary chain technology programme

Auxiliary chain originates from the authorization of the basic block chain, which provides the original evidence and identity, and determines the attributes and parameters of the auxiliary chain through the intelligent contract issued by the basic chain. The main chain, KanBan and storage architecture participate in the verification during the transaction.

Design idea, the main network transmission and data processing as far as possible in the auxiliary chain node execution, but only the necessary evidence and data submitted to the KanBan and open storage system.

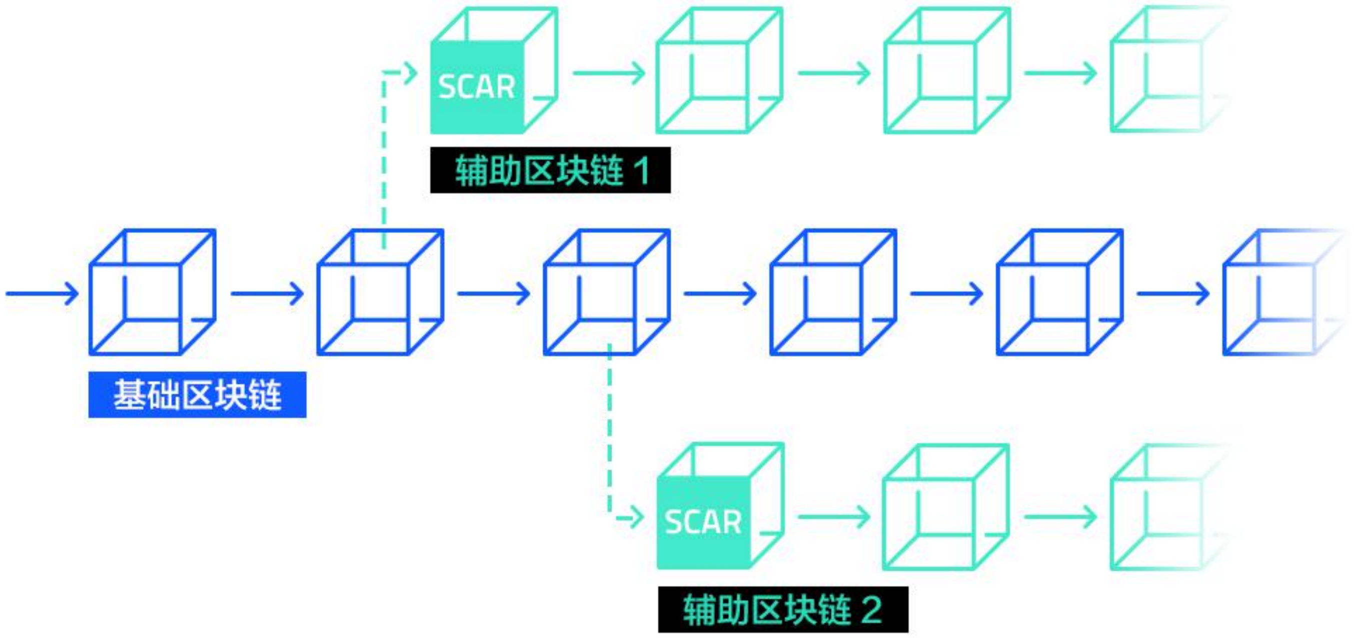


Figure 11. Schematic diagram of auxiliary chain construction

note that the illustrated co-chain is not formed from the main chain bifurcation, and the dashed line represents only dependence.

The auxiliary chain contains the following key elements: initial block, intelligent contract address routing (SCAR), cross-chain unified address (CCUA) protocol and KanBan proof, which guarantee the reliability, security and effectiveness of the auxiliary chain transaction.

the starting block of each auxiliary chain is a special block signed by the base block chain, and a special account is defined for the auxiliary chain, called intelligent contract agent routing (Smart Contract Agent Route, abbreviated as SCAR), to represent the auxiliary chain with all transactions outside.

In the overall design scheme of the system, the auxiliary chain can be two independent block chains generated from the same root, the value chain and the transaction chain, respectively, which can be used to serve the value maintenance and transaction management of the auxiliary chain. As shown below:

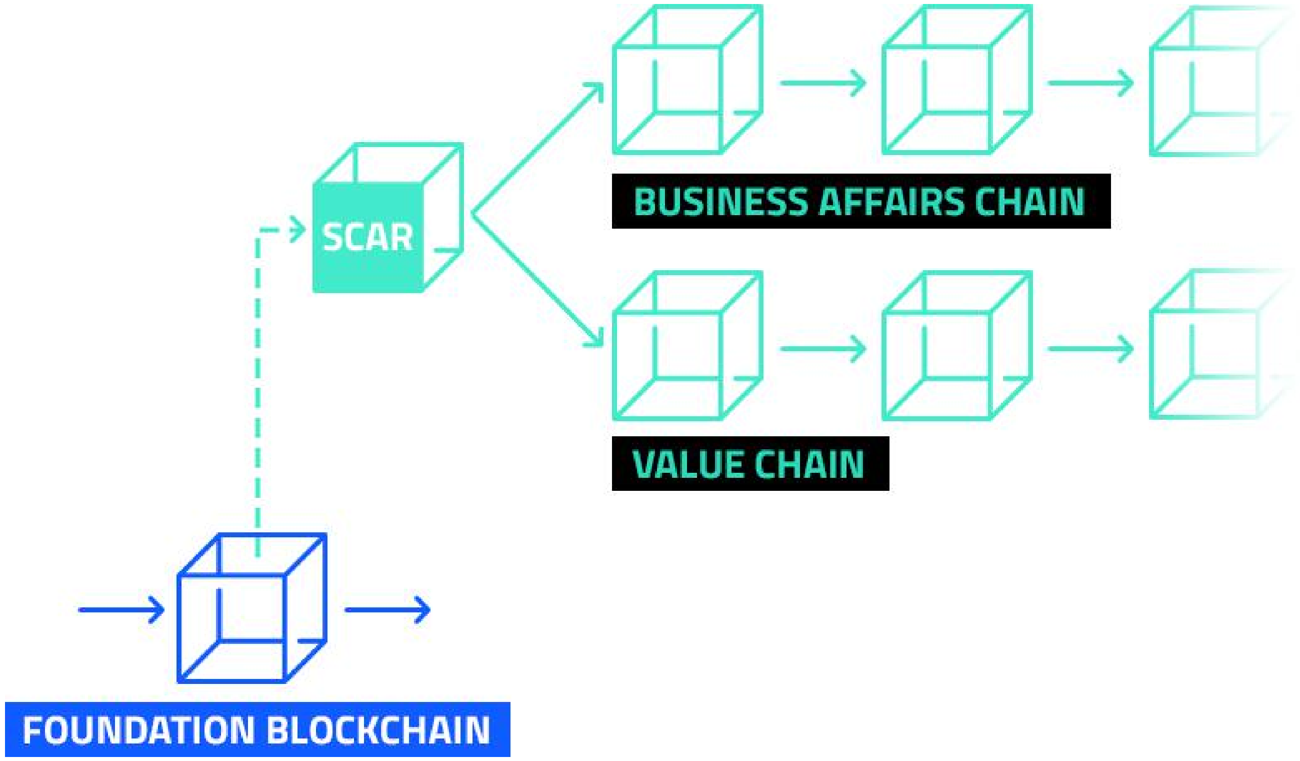


Fig .12. Complete auxiliary chain double-stranded structure

Value chain records value transactions, transaction chain records business logic and business data. This double-stranded mechanism enables the system to build a general functional layer between the underlying block chain and the upper business logic to support all kinds of specific business application requirements.

This programme is limited to the introduction of the value chain, and the transaction chain will be handled separately with the generic functional layer.

In principle, the auxiliary chain adopts the basic block chain value system, that is, directly trading the base chain currency on the auxiliary chain. But in order to make the system more flexible to adapt to various application scenarios, the system design scheme supports customized auxiliary chain protocol and consensus mechanism, allowing users to issue their own independent currency.

2.3.2 Value of Auxiliary Chain and Trust Mechanism Maintenance

The trust mechanism of the auxiliary chain originates from the basic block chain, which is restricted by the basic block chain and its rules, and the result and final decision are attributed to the basic block chain.

Generally speaking, the identity and attributes of the auxiliary chain are determined by the main chain, the validity of the transaction needs to be approved by the main chain, the data storage is required by the main chain, and the final settlement is decided by the main chain. The design principle of the system is that the operation should be carried out by the auxiliary chain node as far as possible.

With regard to the maintenance of value within the auxiliary block chain, it should be treated differently according to the circumstances:

For the auxiliary chain that adopts the base block chain value system, its value mechanism also originates from the base block chain, runs according to the base block chain protocol, specification and consensus mechanism, is bound by the contract signed by the base block chain, is supervised by the base block chain and finally accepts the ruling of the base block chain.

for the auxiliary chain adopting independent value system, its value is not derived from the base block chain, and the transaction outside the auxiliary chain is also restricted, which can only be carried out through local exchange mode. the base block chain does not verify its consensus mechanism, but the base block chain still has the supervisory power and final adjudication power, and the verification rules of the transaction are still formulated by the base block chain through the contract.

2.3.3 The starting block of the auxiliary chain

When the auxiliary chain is initialized, apply for authentication from the main chain to generate the ID、 private / public key pair and attribute contract of the auxiliary chain. These data are stored in the starting block. The system supports the KYC function in an optional manner and can confirm the identity of the auxiliary chain owner (not necessary).

it should be noted that the auxiliary chain ID is different from the node. one node can run multiple auxiliary chains, each of which has its own independent ID and key pairs, and the same auxiliary chain can also run on multiple nodes.

When each auxiliary chain is initialized, at the same time, it generates a unique account authenticated by the main chain. As the agent of the transaction between the main chain and the auxiliary chain, it is called the intelligent contract agent routing (Smart Contract Agent Route, referred to as SCAR), and the SCAR is a special account, which is controlled by the main chain intelligent contract, and has the particularity that no one can operate the account artificially, including the auxiliary chain and the owner of the node. The account can only be executed by the underlying block chain for transactions between its peer accounts with the secondary chain or logically for transactions between the internal accounts of the secondary chain.

Meanwhile, the auxiliary chain ID、 public key and attribute parameters are stored in the KanBan auxiliary chain list.

The starting block of the auxiliary chain is the authorization block issued by the base chain, which contains the verifiable ID, of the auxiliary chain with stubs in the base chain and KanBan.

2.3.4 Auxiliary chain kernel structure

The core structure and most of the functions of the auxiliary chain are the same as the basic block chain, and many modules can even be common. but the consensus mechanism and miner software are different, and the auxiliary chain has more selectivity than the basic block chain kernel module.

Because the auxiliary chain can customize its own currency system and has the function of transaction packet processing and sending open storage architecture data, the auxiliary chain kernel also has the module of package processing, KanBan communication and data exchange, data external storage management module and so on.

A very important special module in the core function of the auxiliary chain is the SCAR processing module to convert all transactions into interactions with the SCAR.

Yi, and maintain the related party transaction status.

Additional secondary storage modules need to extend open storage architecture (OSN) support.

Auxiliary chain, KanBan function is optional, only when there are subordinate subchains. The structure is shown in the figure:

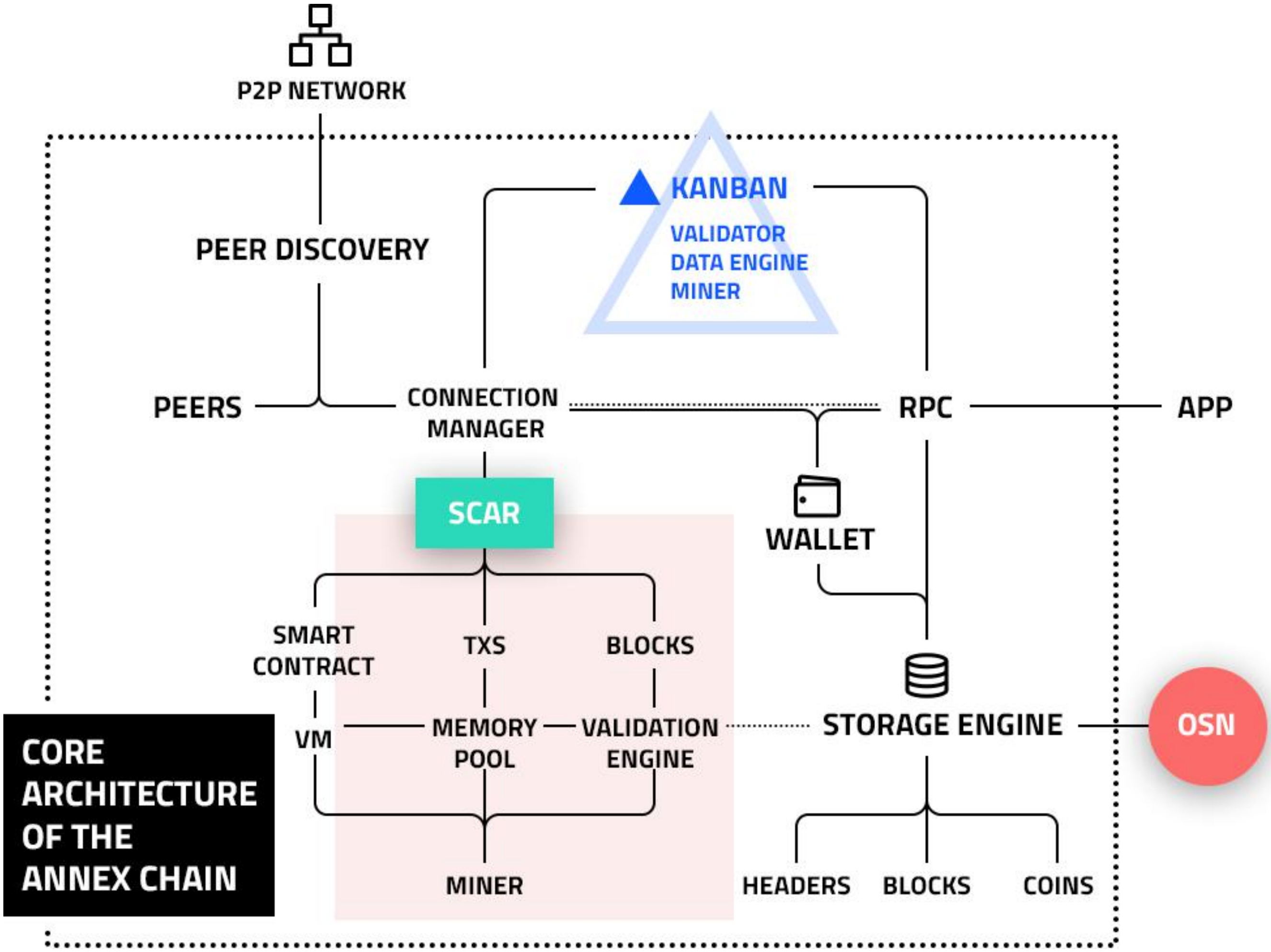


Figure 13. Co-chain kernel architecture

The above figure shows only the value-related co-chain architecture, which has been omitted in system design because the co-chain also supports transaction chains and there are actually more modules.

2.3.5 Address format

This system makes a set of special rules for address design - Cross-chain Unified Address Protocol (Cross Chain Unified Address, abbreviation CCUA)

The same address belongs to the same owner. The specific rules

are as follows: an address consists of four code segments,

namely: address type code - chain code - address code - check

code

The address type code is 2 bytes, the current 0 m is the base

chain PKH address ,1 a is the auxiliary chain PKH address; the

chain code is 4 bytes, representing the number of the chain where

it is located, the base chain number is 0000;

Only the address code is assumed to be the PKH value, and the auxiliary chain and the

base block chain adopt the same private key and public key, so the corresponding

address is the same; the check code is the first 4 bytes after the secondary Hash of

the combined address string.

Any account with the same two address segments belongs to the same owner, regardless of chain, such as:

m 0000aaabbbccc123y4sg

1a 0a4u aaabbbccc123g8rj

0

Both accounts, one located in the base block chain and one located in the auxiliary chain a4u the chain code 0, belong to the same owner because the address code segment is the same.

The secondary chain and the base chain are only traded between addresses of the same owner with the same address code.

When an auxiliary chain user submits liquidation to the underlying block chain, it must go to the corresponding address.

An address on the secondary chain is a transaction status address, that is, each transaction does not change the address, but only updates the balance.

cross-chain unified address protocol CCUA provides convenient means to implement transaction verification and simplify the management of auxiliary chain transactions. in fact, cross-chain unified address protocol is not limited to this system, it can be used as the only cross-chain unified address protocol, which is suitable for all block chains. it can provide very convenient means for the implementation of general decentralized transaction management.

2.3.6 SCAR accounts and transactions

each secondary chain has a special account called the smart contract agent routing account Smart Contract Agent Route, abbreviated SCAR, the control of the account is limited to the smart contract authorized by the underlying block chain to execute the transaction between the underlying chain and the corresponding account of the secondary chain, which is routed.

The smart contract is also established and controlled by the main chain.

SCAR is the secondary chain trading hub. All transactions between the subsidiary chain accounts are converted into transactions between the subsidiary chain accounts and the SCAR, all of which are subsidiary chain accounts Transactions between the chain and the main chain and other auxiliary chains are also executed through SCAR accounts, which streamline all transactions on the auxiliary chain with the aim of reducing the underlying chain transaction data when the user applies for liquidation from the underlying block chain and can be executed without the consent of the counterparty to the transaction, and SCAR also provides possible measures for the base chain to guard against auxiliary chain fraud.

But the transaction is verified by a decentralized KanBan and the data is saved by a decentralized open storage node. The auxiliary chain itself does not have the right of adjudication or the exclusive right of data, so it is completely decentralized.

SCAR account private key of the auxiliary chain is controlled by the main chain intelligent contract.

Any transaction on the secondary chain is checked for legality by smart contracts and SCAR.

transactions between any two accounts on the auxiliary chain are streamlined into transactions between users and SCAR.

Transactions between account A and account B on the secondary chain: conversion of A →B to A A →B SCAR and SCAR A →B B

Voice transaction between secondary chain account A X main chain

account: A →X conversion X1→SCAR and SCAR X1→SCAR X transactions

between the main chain account X and the secondary chain account: X

X1→SCAR A conversion to X X1→SCAR SCAR, SCAR →X1 and X1SCAR →X1A

transactions between user AB of different auxiliary chains: A →B

conversion to A A →B SCAR1,SCAR1A →B SCAR2 and SCAR2A →B B KanBan always

maintain the total state of each auxiliary chain, and can be accounted for

by the collection UTXO auxiliary chains.

2.3.7 Secondary chain trading status

The system establishes four states for the effective transaction of auxiliary chain, namely: executed, witnessed, confirmed, completed, representing four different transaction processes.

When the secondary chain receives the transaction, it executes locally, generates the transaction, which is the executed state of the transaction, usually completed in milliseconds, which is only the transaction within the secondary chain. If the secondary chain is a single full node chain, it is equivalent to the current centralized transaction, and the credibility of the transaction in this state is equivalent to the credibility of the secondary chain;

The secondary chain submits the transaction package to the KanBan, and receives KanBan confirmation, which is a witness state, usually completed in seconds to minutes. When submitted to the KanBan,, the transaction status is maintained by the KanBan, and the trustability is greatly enhanced. However, as submission to KanBan is an auxiliary chain submission not propagated by the main chain P2P the network, so the KanBan is recognized as a numerical parameter, representing the number of confirmed KanBan, the higher the number, the more reliable;

The secondary chain is generated in blocks and stored KanBan a visa and delivered to an open storage node, known as confirmed, usually completed in a few minutes. Submission to an open storage architecture indicates that data storage is decentralized and transactions are already very trustworthy. Similar to KanBan, the more open storage architecture (OSN) nodes are submitted, the higher the trustworthiness;

when the user submits the liquidation to the underlying blockchain and is completed, for the completed status, depending on when the user submits it. In this case, the account-related transactions have been submitted to the main block chain. with the highest level of trust.

Usually the transactions that have witnessed the state are basically risk-free transactions, the general small transactions can be regarded as reliable; only the confirmed state of the transaction has sufficient security guarantees, the larger amount of transactions can be assured.

Because the trustworthiness of the witness state is determined by the number of KanBan, and the trustworthiness of the confirmed state is determined by the number of storage nodes submitted, the system provides a special interface to provide a simple judgment means for the client through the intelligent contract.

2.3.8 Auxiliary chain transaction processing process

The secondary chain value transaction pr

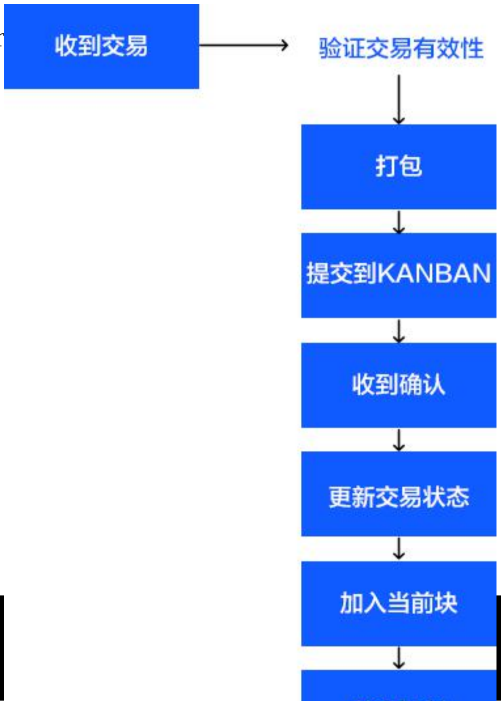


Figure 14.
Auxiliary chain value transaction processing process

Supplementary transactions need to be verified by KanBan, which is necessary to prevent double flower attacks, and only transactions that pass KanBan verification and receive KanBan signature stubs are valid.

After receiving the packet submitted by the auxiliary chain, the main chain verifies the packet, first verifies the body, then verifies the validity of the packet, finally verifies the validity of the record in the packet, if there is a problem to reject and notify the auxiliary chain, if verified, changes the status of the KanBan related record, puts the transaction in the outstanding transaction form, and signs for receipt, sends the receipt to the auxiliary chain;

After receiving the rejection from the main chain KanBan, the auxiliary chain shall remove the suspicious transaction and repackage the submission.

The secondary chain and KanBan packet data and transaction records should be kept in exactly the same order and time records, each sending packet contains the Hash value of the previous packet. This minimizes data transmission, and when all nodes generate blocks through the PoS, simply inform the parties of the Hash value of the last package.

Generally, the underlying chain KanBan a packet that receives the secondary chain and contains one or more transactions;

The transaction is globally valid after receiving KanBan node verification, and the more KanBan node confirmation received by a secondary chain transaction, the higher the credibility.

The transaction in the auxiliary chain is sent to the KanBan node independently after the auxiliary chain is packaged, and the communication between KanBan nodes is no longer automatically P2P between nodes.

2.3.9 Block Process for Auxiliary Chain

the auxiliary chain, blocks are generated by a POS consensus mechanism involving the auxiliary chain nodes, KanBan、 open storage nodes, and can be verified by KanBan or storage framework.

client confirms that the block is valid if the block is verified by validity, the block or its downstream block is signed by the KanBan, and the block data is saved at the open storage node.

Transactions in the auxiliary chain are sent to the KanBan node by the auxiliary chain packaging, and the KanBan nodes are no longer broadcast automatically.

when a block of an auxiliary chain is generated according to its consensus mechanism, it will be propagated between the nodes of the auxiliary chain p2p network. the transmitted data includes nonce, last packet id and the nodes involved in the merkle root,p2p network in the new block include all the full nodes, participating KanBan and participating nodes of the auxiliary chain.

After block locking in the secondary chain, block data is broadcast to the open storage node.

2.3.10 Auxiliary Chain Double Flower Attack

The design of this system can effectively eliminate the double flower attack of auxiliary chain.

First, in the case of the auxiliary chain honest, the intra-chain attack can not be implemented, the status of each account on the same auxiliary chain can be obtained from the local real-time, there is no intra-chain attack vulnerability;

If the secondary chain is specifically designed for fraud, the client verifies the validity of the transaction by providing KanBan and open storage nodes. The verification mechanism of the KanBan and open storage architecture can determine whether it is client fraud or auxiliary chain fraud, if it is client fraud, the transaction is invalid, if it is auxiliary chain fraud, apply to the basic block chain to enforce the prohibition of intelligent contract, freeze the transaction SCAR the special account of the auxiliary chain, and initiate an inventory process to check the details of all outstanding transactions in the auxiliary chain;

For the double flower attack between the auxiliary chain and the base chain, the double flower attack between the auxiliary chain and the base chain can not be carried out as long as the double flower attack on the auxiliary chain is eliminated because the system limits the transaction between the base chain and the auxiliary chain.

Double flower attack is a double flower attack between two or more different auxiliary chains. There are several situations to consider:

a) All the supporting chains involved are honest and only the account node attacks:

If the transaction can not be verified by the KanBan and storage system, the whole node and client can get the transaction status in time, and the transaction fails.

b) Part of the subsidiary chain involved in the transaction dishonest double-flower attack:

Clients can verify the validity of transactions through KanBan and storage systems, not only through auxiliary chain nodes. If fraud is considered, the client may also inform the base chain, which performs verification and prohibition;

c) The two auxiliary chains involved in the transaction are dishonest double-flower attacks:

Client can be verified by KanBan and open storage architecture. Indeed, because of the establishment of SCAR and SCAR channels, the more auxiliary chains the transaction crosses, the more loopholes, and the more difficult fraud is to implement.

From this we can see that KanBan and open storage architecture play a vital role in preventing double flower attacks.

Besides, the list of auxiliary chains in the KanBan records the starting time of auxiliary chains and the total amount of transactions, which can be used as credit parameters of auxiliary chains for client reference.

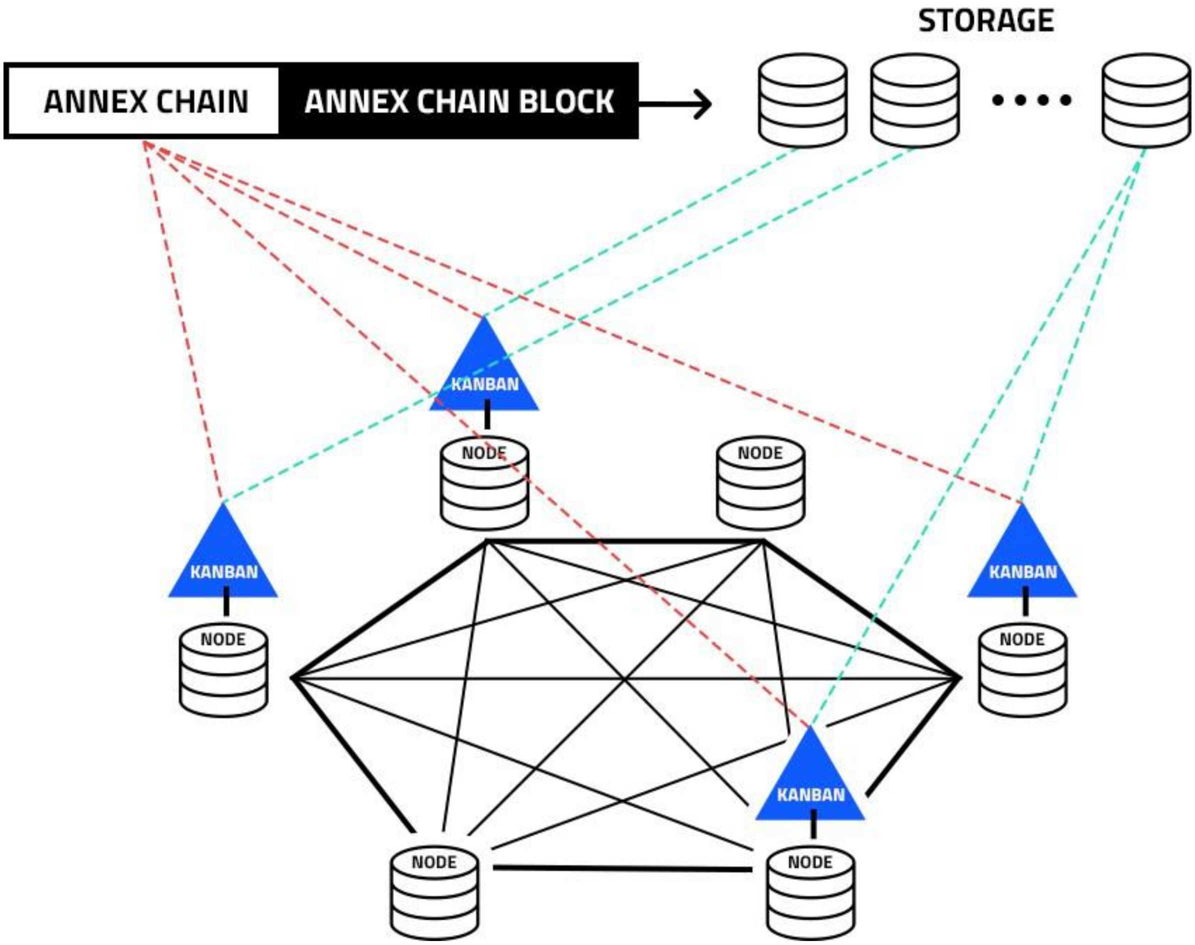


Figure 15. Verification diagram of the whole system

2.3.11 Liquidation of subsidiary chain accounts

the value transaction of the auxiliary chain has global validity, which is implemented through KanBan function and a decentralized storage architecture, that is, the account status of the auxiliary chain is always synchronized with the KanBan, and the block containing the transaction record is submitted to the storage node storage specified by the KanBan.

When the auxiliary chain customer submits the account liquidation to the base block chain, even if the auxiliary chain in which it is located disappears, the liquidation can be carried out smoothly because the KanBan and storage system holds complete transaction data and status information, and because of the establishment of the SCAR mechanism, any auxiliary chain transaction is transformed into a transaction between the user and the SCAR, and the SCAR is controlled by the base block chain, so the liquidation can be carried out without the consent of the other trading parties.

After the liquidation is completed, the corresponding address on the auxiliary chain is emptied, and the corresponding record in the KanBan is also deleted.

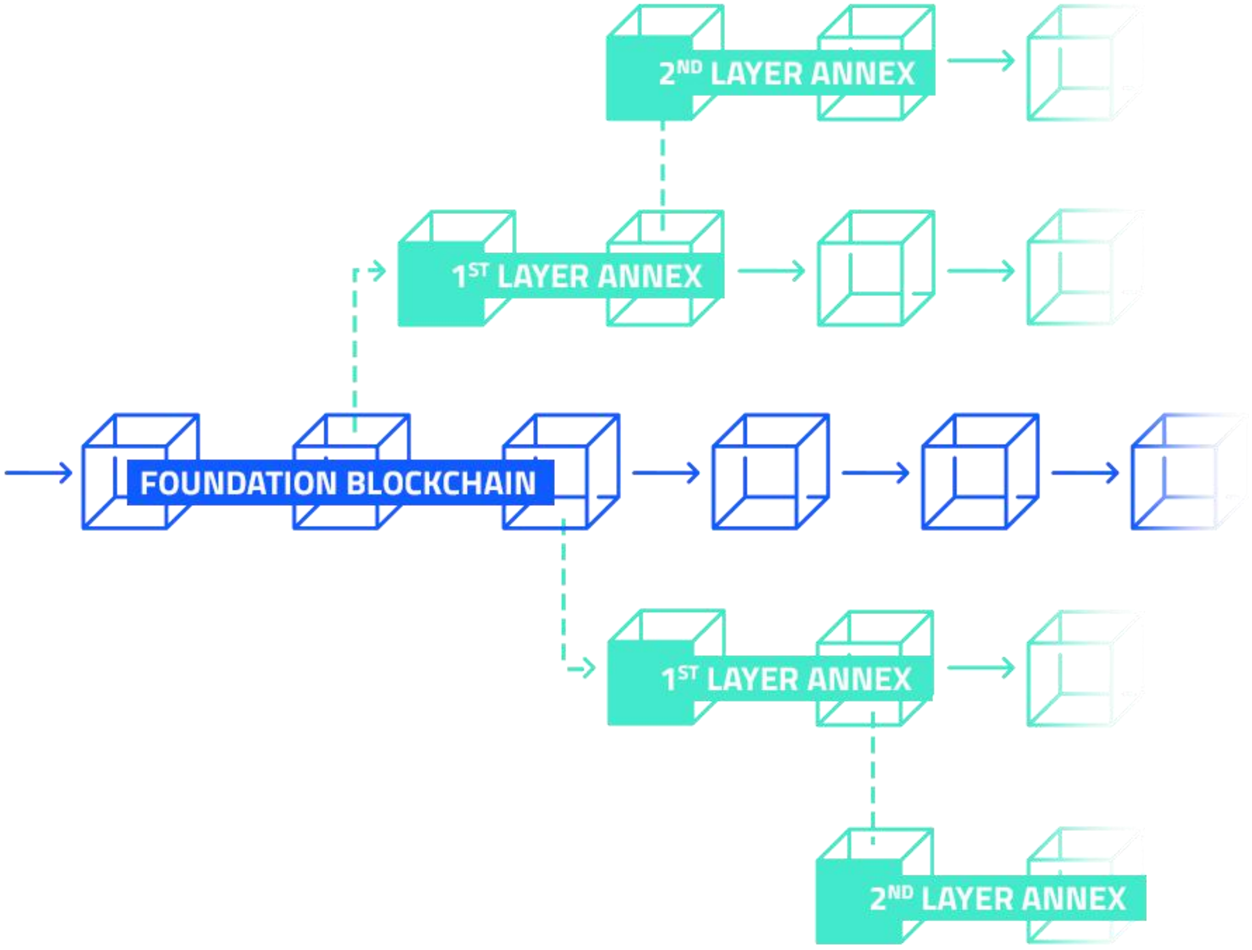


Figure 16. Hierarchical auxiliary chain structure diagram

2.3.12 Auxiliary Chain Hierarchical Architecture

The auxiliary chain is not limited to one layer in system design principle, but can build multi-level chain. As shown below:

The so-called multilayer auxiliary chain structure is to derive the next auxiliary chain from the auxiliary chain, the upper chain is called the parent chain, and the derived chain is called the sub chain.

in a hierarchical auxiliary chain system, the KanBan of the child chain is maintained by the parent chain node. therefore, the auxiliary chain core also has KanBan modules that configure activation if necessary.

Because the first byte of the four bytes in the block chain coding part of the system is used to express the depth, the remaining three bytes are used as the chain number, so the whole system can have a maximum of 256 auxiliary chains, and each level can have a maximum of 16,777,216 auxiliary chains.

2.3.13 Auxiliary chain value system and consensus mechanism

In general, the auxiliary chain adopts the same value system of the base block chain, that is, the currency transaction of the base chain is executed directly in the auxiliary chain, the condition is that all the chains of the auxiliary superior adopt the base chain value system.

This system supports the user-defined value system and consensus mechanism of auxiliary chain, and its purpose is to enhance the flexibility and adaptability of the system. For reasons of business needs, an auxiliary chain can issue its own currency and maintain its own independent value system.

Father chain KanBan still maintain the state of child chain transaction, if the child chain and the main parent chain are the same value system, the child chain and the parent chain can be freely traded, and if the child chain and the parent chain are different value systems, the value conversion can only be realized through the exchange mechanism of the same level transaction.

2.4 Open storage architecture

The open storage architecture of Beidou block chain system is one of the three components of the system, and the open storage mechanism is very important to build a decentralized commercial application.

2.4.1 Open Storage Architecture Design

open storage architecture fully supports the value transaction and transaction record storage of the beidou commercial blockchain, and uses MapReduce technology to construct mapping to streamline the function model to support big data fast query.

Open storage architecture not only supports fast query for block chain transactions, but also supports fast query of content-based open business information related to transaction block chain, which serves the system and lays the foundation for the establishment of search engine in block chain era.

The system is designed to attract service providers to join the system actively with the benefit incentive mechanism: first, the system pays the income of storage expenses; second, it supports the decision of POS consensus mechanism through the MapReduce function to participate in the auxiliary chain to obtain the mining income; third, the public open business data is the block the basis of chain age search engines.

For supporting big data concurrency, the system architecture design scheme is to adopt Sharding technology in the database port layer to support the horizontal expansion of the database.

The overall logical architecture of the storage system is as follows:

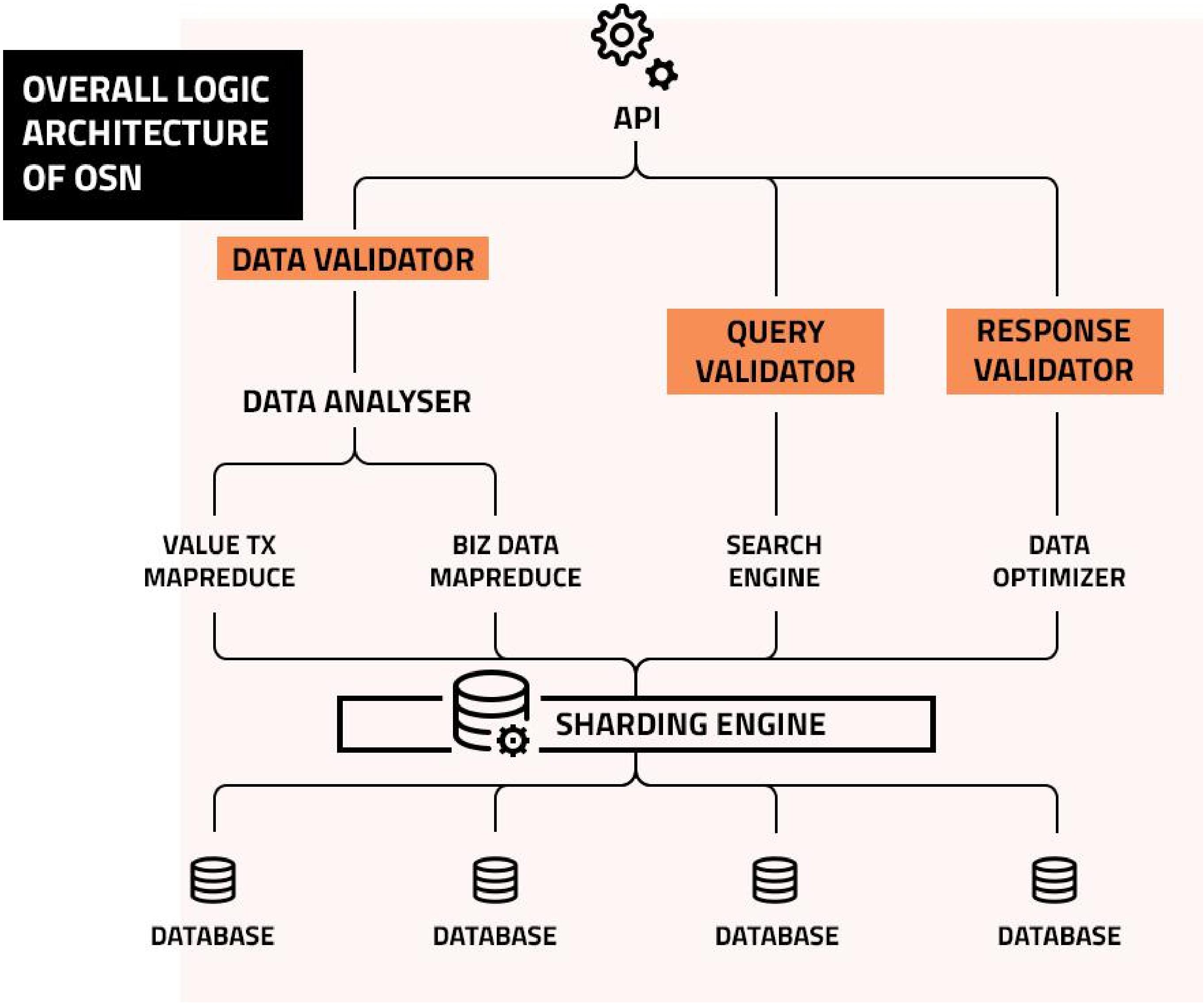


Figure 17. General logical architecture of storage systems

The design of the whole storage system is the same as the public block chain system, using an open architecture, service providers and users are free to join.

2.4.2 Storage node kernel architecture

Besides the data storage architecture, the nodes of the open storage architecture also have P2P protocol compatible with the block chain system and the connection management and communication interface, which can easily join the block chain network.

Storage nodes also participate in the consensus mechanism of each auxiliary chain through P2P network.

An open storage node may be associated with multiple secondary chains, providing data storage services for multiple secondary chains and participating in consensus mechanisms for multiple chains. The storage node architecture diagram is as follows:

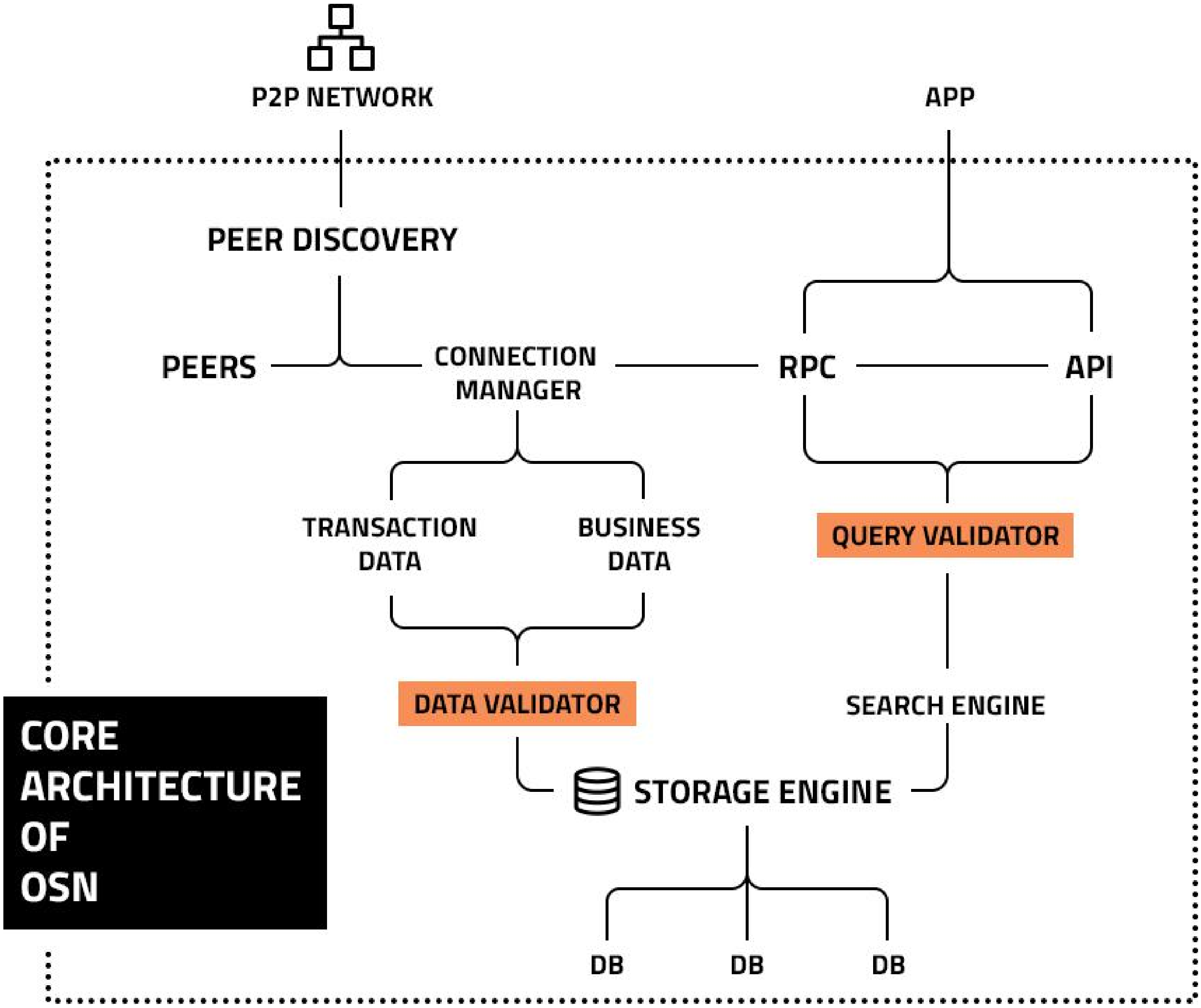


Figure 18. Open storage node kernel architecture

2.4.3 Cost incentive mechanism for storage nodes

The cost mechanism of the storage node is formulated by the intelligent contract of the base block chain. In principle, the storage node can freely formulate the storage cost, but the cost is added as a parameter POS the rule of consensus mechanism is determined, the higher the cost, the lower the voting right of the POS, the formula of voting right is:

$$W = V / R$$

Among them: W - voting weight;

V - voting

weights; R -

storage rates.

Direct revenue from storage nodes includes storage costs and POS mining revenue, and potential revenue includes data search services.

3. value system

The Beidou commercial block chain system adopts the unified basic monetary system, Beidou coin (T B D), which is the abbreviation of English TheBigDipper. Beidou coin, as the value basis of the system, is used in all three parts of the system, and is the standard value unit for all expenses and value exchange.

A total of 21 million coins were issued on a quantitative basis, of which 3 million were reserved for development and promotion incentives ,2 million were issued through EOS exchange, and the remaining 16 million were produced through mining, and the mining mechanism for issuing coins was launched in August 2020.

R & D team

Founder CEO, Zhang Hui

Singapore Chinese, graduated from Peking University, more than 20 years of technical R & D management experience, long-term engaged in IT architecture design, IT Consulting work. In recent years, focusing on the research of business model of digital currency and block chain, the concept of "block chain business analysis" has been put forward for the first time, and currently serves as a technical tutor of block chain in many financial institutions and educational institutions.

2019" china cloud computing conference "blockchain technology summit speaker.

Allan Man co-founder

Hong Kong blockchain technology development and application experts, long-term in government departments engaged in network security and identity information management.

CTO, core developer

华为 former senior R & D manager, proficient in JAVA and other development languages, has written more than 100,000 lines of block chain underlying code.

Benny password design, core developer

International famous cryptography experts and white hat hackers, long engaged in the design and attack of Hash functions, security encryption chip hardware and software algorithm design, the inventor of multiple core algorithms.

References

1. A method of validating external data block by Bitcoin transaction to construct new blockchain,Paul Liu

2. Using Smart Contract Account Routing to Streamline Transactions, Paul Liu

3. A method of constructing scalable blockchain by using KanBan to update off-chain state,Paul Liu

4. Bitcoin：A Peer-to-Peer Electronic Cash System,Satoshi Nakamoto

5. The Business Blockchain－promise,practice and application of the next internet technology,William Mougayar

6. Omni Layer Specification,https://github.com/OmniLayer/spec

7. Enabling Blockchain Innovations with Pegged Sidechains,Adam Back et al

8. Blockchain －Blueprint for a new economy,Melanie Swan

9. Mastering Bitcoin,Andreas M.Antonopoulos,O'REILLAY,First Edition,December 2014

Disclaimer

This White Paper is intended to convey information only and the contents of the document are for reference only and do not constitute any investment offer, solicitation or solicitation for the sale of digital goods, stocks or securities. Such solicitation must take the form of a confidential memorandum and be in accordance with the relevant securities and other laws. The contents of this document shall not be interpreted as forcing participation to swap. No act relating to this white paper shall be deemed to be involved in the exchange, including the requirement to obtain a copy of this white paper or to share this white paper with others. Participation in the swap represents that the participants have reached the age standard, have complete civil capacity, and the contract with the Beidou chain Foundation is true and effective. All participants signed the contract voluntarily and had a clear and necessary understanding of the Beidou chain before signing the contract.

The Beidou Chain Foundation will continue to make reasonable attempts to ensure that the information in this white paper is true and accurate. During the development process, the platform may be updated, including but not limited to the platform mechanism, token and its mechanism, token distribution. Part of the document may be adjusted as the project progresses in the new white paper, the Beidou chain foundation will be published on the website or the new version of the white paper, etc. Participants are requested to obtain a new version of the White Paper in a timely manner and to adjust their decisions in a timely manner according to the updated content.

The Beidou Chain Foundation does not cover participants because:

(1) Depend on the content of this document

(2) Inaccurate information in this paper

(3) loss caused by any act caused by this paper.

The BeiDou Chain Foundation will spare no effort to achieve the objectives mentioned in the document, however, based on the existence of force majeure, the BeiDou Chain Foundation can not make a complete commitment.