Open▲

WHITE　PAPER

File Name ： perfect decentralized and closed cycle
block chain Crowd Ecological System

NO. ：

Version ： 1.6

Contents

1 SUMMARY..4

2 TERMS, DEFINITIONS AND ABBREVIATIONS..5

2.1 TERMS, DEFINITIONS..5

2.2 ABBREVIATIONS..5

3 BACKGROUND..5

3.1 BLOCKCHAIN CURRENT PROBLEM..6

3.2 APP/DAPP CLAIM..6

3.2.1 *Support hundreds of millions of users*..6

3.2.2 *Easy to use*..6

3.2.3 *User use painless*..6

3.2.4 *Easy upgrades and bug fixes*..6

3.2.5 *Low latency*..6

3.2.6 *Sequential*..6

3.2.7 *Concurrent performance*..7

3.2.8 *Fast access*..7

3.2.9 *Scene diversity*..7

4 CES..7

4.1 CONSTRAINT AND ACCESS SYSTEM..7

4.1.1 *Constraint*..7

4.1.2 *Access system*..7

4.2 TECHNICAL ARCHITECTURE..8

4.2.1 *C2I based module package*..8

4.2.2 *Ecosystem model diagram*..8

4.2.3 *Ecosystem Pentagram Architecture*..9

4.2.4 *Application model diagram*..9

4.2.5 *Blockchain*..10

4.3 BUSINESS ECOLOGY..14

4.3.1 *Main chain*..14

4.3.2 *Payment chain*..14

4.3.3 *Credit chain*..15

4.3.4 *Certification chain*..15

4.3.5 *Notary chain*..15

4.3.6 *Industry chain*..15

4.3.7 *Small quick payment (mobile payment)*..15

4.3.8 *Patronus and guardian Elf*..15

4.4 DIGITAL CURRENCY..18

4.4.1 *Security fund*..18

4.4.2 *Contribution fund*..19

4.4.3 *Give away rewards*..19

4.4.4 *Stationed chain reward*..20

4.4.5 *Stationed APP reward* 20

4.4.6 *Airdrop* 20

4.5 Ecological governance 20

4.5.1 *Freeze and unfreeze accounts* 20

4.5.2 *Change account legal person key* 20

4.5.3 *Organize EIP voting* 21

4.5.4 *Stationed chain resource allocation* 21

4.5.5 *Cash contribution award* 21

4.5.6 *Emergency change* 21

4.6 Module management 21

4.6.1 *Module release* 21

4.6.2 *Module check* 21

4.6.3 *Module update* 21

4.7 Node classification 21

4.7.1 *Classified by performance* 21

4.7.2 *Classified by function* 22

5 SHARDING 22

5.1 Sharding by region 23

5.2 Semi-random sharding by algorithm 23

5.3 Full random sharding by algorithm 23

6 CONSENSUS ALGORITHM 23

6.1 Algorithm implementation 23

6.1.1 *BFT-PCS(A)* 23

6.1.2 *BFT-PCS(B)* 25

6.1.3 *BFT-PCS(C)* 25

6.2 Algorithm Features 26

6.3 Transaction confirmation 27

7 ACCOUNTS 27

7.1 Actions and Handlers 27

7.2 Role Based Permission Management 28

7.2.1 *Permission Mapping* 28

7.2.2 *Parallel Evaluation of Permissions* 28

7.3 Double key protection 29

7.4 Stolen account recovery 29

8 SCRIPTS AND VIRTUAL MACHINES 29

8.1 Schema Defined Action 29

8.2 Schema Defined Database 29

8.3 Generic Multi Index Database API 30

8.4 Separating Authentication from Application 30

8.5 Code is separated from the instance 30

8.6 WASM 30

9 COMMUNICATE WITH THE BLOCKCHAIN NODE.. 31

9.1 TRANSACTION DELAY.. 31

9.2 PROOF OF INTEGRITY.. 31

1 Summary

CES: perfect decentralized and closed cycle block chain Crowd Ecological System，Here in after referred to as "this ecology" or "this ecosystem".

By designing a new technology architecture based on cloud computing, CES can carry blockchains from all walks of life, forming a blockchain ecosystem that achieves complete decentralization and closed loop without any external conditions. This ecosystem will try to remove the command line operation mode and provide graphical operations for all users in each link.

The blockchain has solved the trust problem, and the ecosystem will focus on credit, certification, notarization and payment issues.

CES has 9 major innovations:

1) A new technical framework that carries a blockchain group that is symbiotic and prosperous in all walks of life;

2) Complete decentralization (only the underlying blockchain, excluding the upper application) and the closed-loop blockchain ecosystem;

3) The first consensus algorithm for multiple-sharding multiple-consensus, TPS meets the requirements of large-scale commercialization;

4) The first dual key protection mechanism, the account assets are more secure;

5) The payment chain that comes with the ecology supports the legal currency - legal currency, legal currency - digital currency, digital currency - digital currency trading, no longer dependent on any external exchange;

6) Shared business ecosystem (shared users, markets, technologies, application solutions), and has a huge advantage to attract developers to develop applications and smart contracts based on this ecosystem;

7) Universal and unique accounts and digital currencies (excluding tokens) throughout the blockchain ecosystem;

8) Data is treated differently, and a zero-knowledge proof algorithm is introduced to protect the privacy data that needs to be protected;

9) Can quickly develop the industry chain and issue their own tokens, no longer have "air coins";

2 Terms, definitions and abbreviations

2.1 Terms, definitions

术语	英文	含义
架构	Architecture	也叫体系结构
云计算	Cloud Computing	云计算
实例	Instance	类实例化（instantiated）后的实体

2.2 Abbreviations

缩略语	英文	含义
API	Application Programming Interface	应用程序接口
APP	Application Program	特指传统的中心式应用程序
BaaS	Blockchain as a Service	区块链即服务
BFT	Byzantine Fault Tolerance	拜占庭容错算法
DAPP	Decentralized Application Program	分布式应用程序
DAO	Decentralized Autonomous Organization	去中心化的自治组织
DPoS	Delegated Proof of Stake	委托权益证明算法
EIP	Ecosystem Improvement Proposals	生态系统改进建议
EOS	Enterprise Operation System	区块链商业操作系统
ETH	Ethereum	以太坊
IaaS	Infrastructure as a Service	基础设施即服务
ICO	Initial Coin Offering	首次币发行
IPFS	Inter Planetary File System	星际文件系统
KYC	Know Your Customer	了解您的客户
LCV	Light Client Validation	轻客户端验证
PIN	Personal Identification Number	个人识别码
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错算法
PaaS	Platform as a Service	平台即服务
SPV	Simplified Payment Verification	简单支付验证
TPS	Transaction Per Second	每秒交易数

3 Background

Since the birth of blockchain technology, it has been strongly supported by many companies and people. Everyone is looking forward to an ideal world that is completely decentralized, open and transparent, data can not be tampered with, traceable, and community decision-making. However, after Bitcoin, ETH, EOS, the blockchain technology has progressed step by step, but there are still various problems.

3.1 Blockchain current problem

1) Limited performance, failing to meet the requirements of large-scale commercialization;

2) There is no correlation between chain and chain, and it is impossible to co-exist and share prosperity. On the contrary, vicious competition often occurs;

3) Profit-seeking funds like to rebuild new chains for ICO, or just issue “air coins”, and various blockchain are flooding;

4) It relies heavily on external exchanges, and most exchanges are centralized and have low security, which is contrary to the original intention of the blockchain;

5) There is no commercialized and closed-loop blockchain ecosystem;

6) The consensus mechanism still needs further improvement and complete decentralization;

7) Cross-chain and sidechain technologies are immature;

8) Not rich in applications;

3.2 APP/DAPP Claim

3.2.1 Support hundreds of millions of users

Large-scale commercialization needs to deal with the data generated by billion-level users, so supporting a large number of users is crucial.

3.2.2 Easy to use

Large-scale commercialization means that most of the users are ordinary people, and the level of education is general. This requires a commercial model and various user operations, which must be simple and convenient, suitable for the general public, and convenient for global promotion.

3.2.3 User use painless

As the saying goes, "Wool is on the sheep," any cost will eventually be invisibly transferred to consumers. But blockchain technology has greatly reduced costs, and users only have to pay a very low painless transaction fee.

3.2.4 Easy upgrades and bug fixes

Applications need to flexibly enhance applications with new features and solve bugs in the operation and maintenance process.

3.2.5 Low latency

A good user experience requires no more than a few seconds of reliable feedback, and too long a delay can affect the user experience.

3.2.6 Sequential

Some applications must have a sequential order of commands.

3.2.7 Concurrent performance

Large-scale applications require a workload between multiple CPU and computers, or load balancing across multiple service nodes.

3.2.8 Fast access

The application hopes that the underlying blockchain can provide API for multiple development languages for quick access.

3.2.9 Scene diversity

Applications only need to be based on a set of API development provided by this ecosystem, which can greatly enhance the application scenarios by using the functions provided by the blockchain of various industries.

4 CES

4.1 Constraint and access system

This ecology will elaborate the binding and access system in detail, and all ecological chains, applications and users need to comply.

4.1.1 Constraint

Such as prohibiting yellow gambling, prohibiting any external exchange on the token, and so on.

This part is followed by refinement.

4.1.2 Access system

4.1.2.1 Stationed chain

Public chains generally need to have a large influence and a large number of users, or have a public welfare nature, such as household registration, industrial and commercial registration, real estate registration, medical services, intellectual property, charity and so on. The public chain needs to apply, and the purely commercial public chain allows for exclusivity for a period of time.

The alliance chain and the private chain are not required. When a coalition chain or private chain reaches a certain influence, it can apply for a public chain.

This ecology does not charge any fees for all the chain of entry, and the public welfare chain can also receive technical support.

4.1.2.2 Stationed APP

The ecosystem comes with an app store that allows developers to publish their own distributed applications (DAPP) and central applications (APP), as well as smart contracts, and is basically free, as long as they follow the autonomy of the ecosystem.

4.2 Technical Architecture

4.2.1 C2I based module package

All modules in this ecosystem will adopt the C2I encapsulation mode.

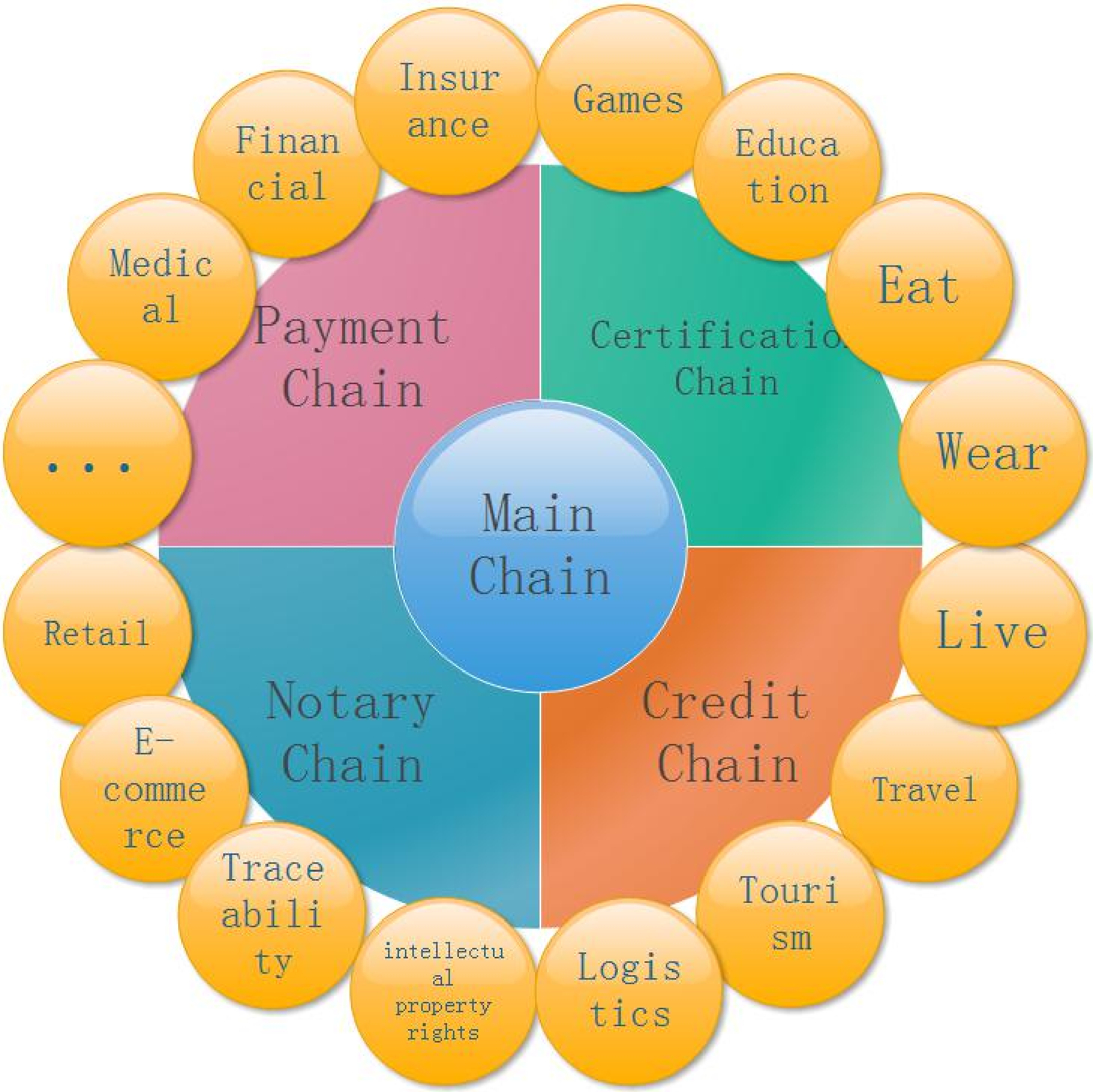
C2I：Class to Interface,Class is Derived from Interface. It is derived from the principle of dependency inversion and interface isolation in the six design principles. Combined with the five major creation modes, bridging mode, and class inheritance, it is the best module encapsulation form obtained in practice.

C2I project：

https://github.com/sunnygood/CEN-XFS

4.2.2 Ecosystem model diagram

With the main chain (account), payment chain, certification chain, credit chain and notary chain as the core, combined with the industry chain of all walks of life, it forms an inter-dependent, symbiotic and co-prosperous blockchain ecosystem.

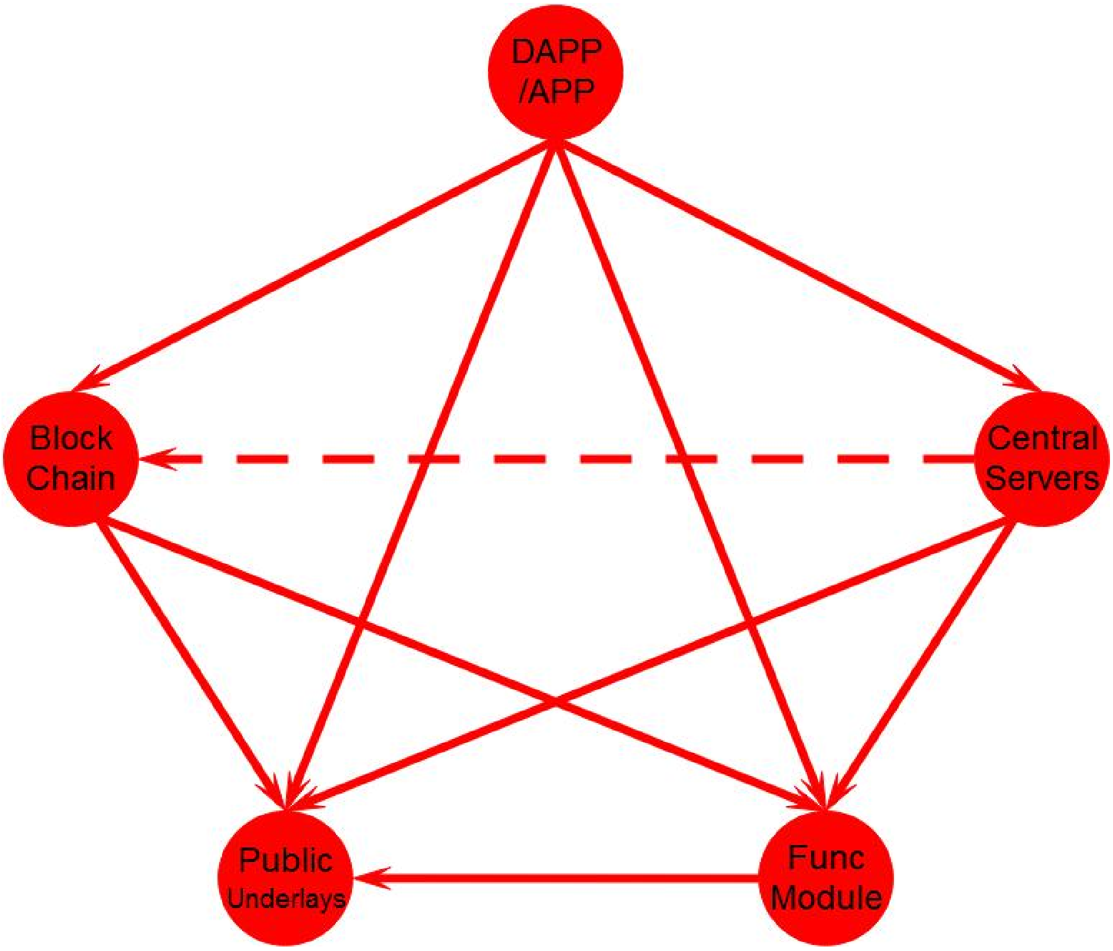


4.2.3 Ecosystem Pentagram Architecture

Most of the existing applications in the world today consist of several (1 to 4) parts of the APP layer, functional modules (services), central servers, and public underlays.

Since the birth of the blockchain, the blockchain is composed of four parts: DAPP layer, functional module (service), distributed blockchain, and public bottom layer. People think that only DAPP can participate in the blockchain ecology. However, due to the distributed nature of DAPP, a large part of the industry is difficult to implement DAPP, coupled with the low participation of developers, resulting in the lack of blockchain applications.

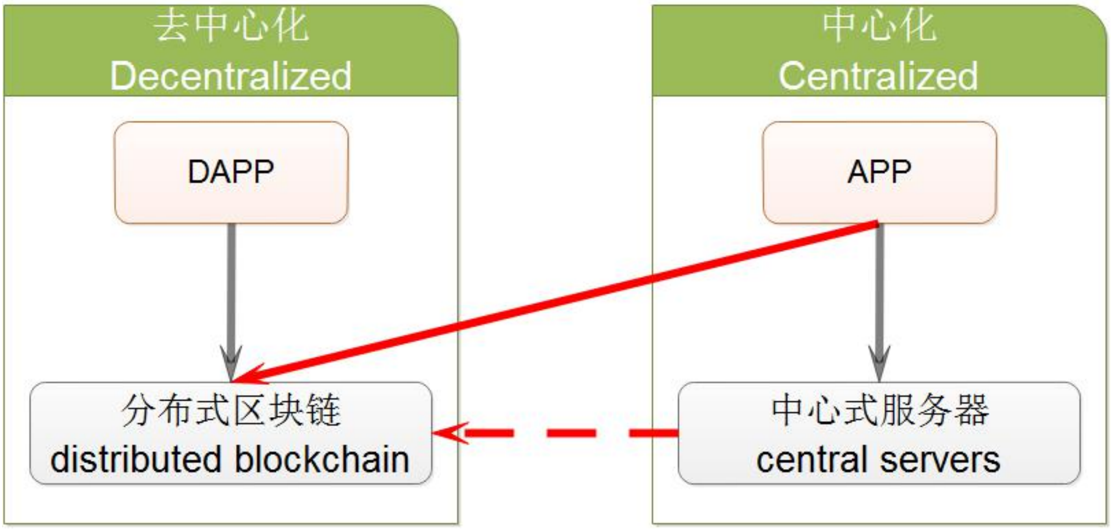
Because of this, this ecology introduces the five-pointed star architecture. As long as the APP uses part of the industry chain, it can combine the decentralized blockchain and the centralized server to make full use of the existing resources and greatly enrich the ecology.



4.2.4 Application model diagram

This ecosystem only pursues the complete decentralization of distributed blockchains. For the application, it can be a decentralized distributed DAPP or a centralized APP, which is determined by the developer.

As shown in the following figure: The left side is a completely decentralized distributed blockchain ecology, and the right side is the centralized application ecosystem that currently occupies a very high proportion. It is through the red arrow in the figure below that the centralized APP can access part of the chain (such as the main chain, the payment chain, the certification chain, the credit chain, the notary chain, the traceability chain, etc.), so that the current world can be Some mainstream applications are included in this ecosystem, enriching the application ecology.



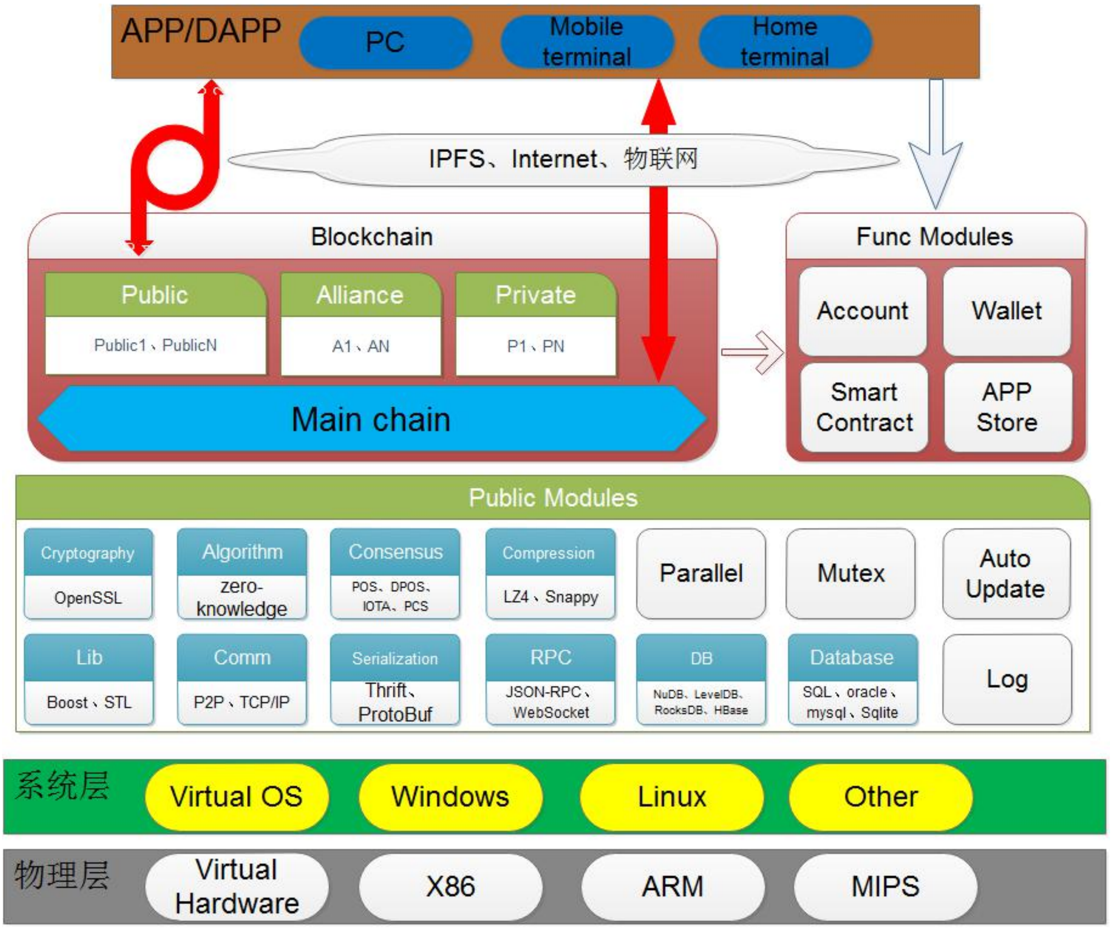
4.2.5 Blockchain

4.2.5.1 Hierarchical diagram

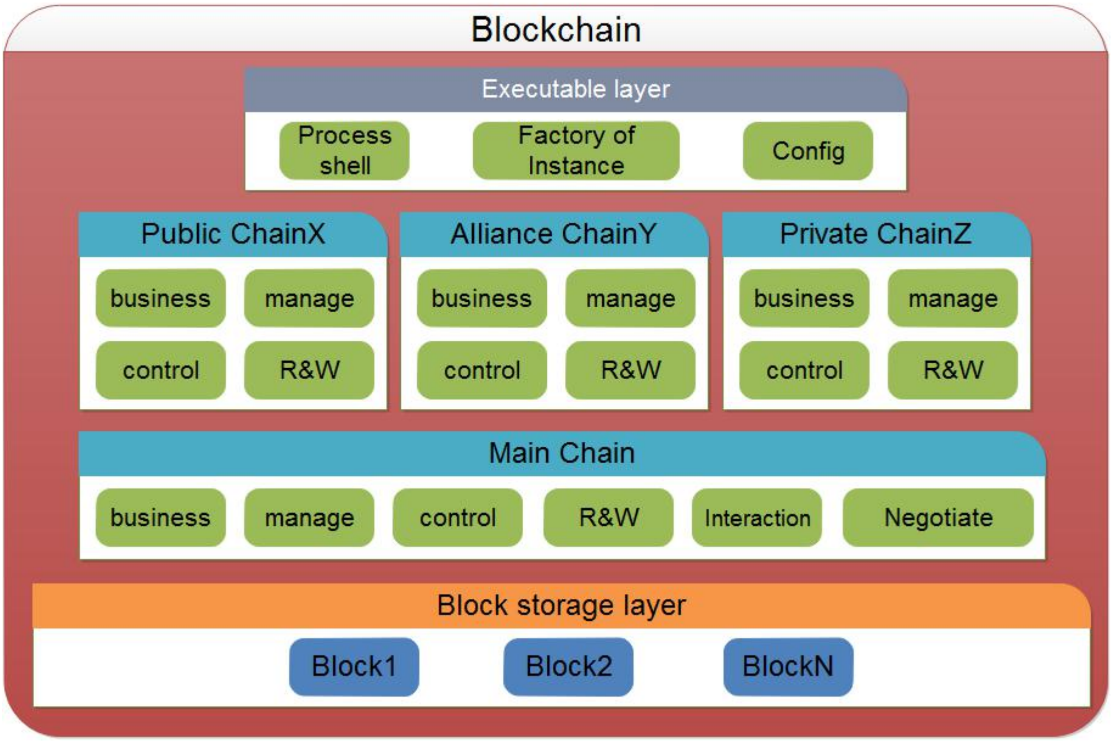
As shown in the following figure, this ecosystem can design a blockchain technology that combines cloud computing to carry blockchains from all walks of life, forming a zone that is completely decentralized and closed without any external conditions. Blockchain ecosystem. The blockchain layer of this ecosystem can enable all chains to run in parallel to achieve interconnection.

In this ecosystem, the application can be a central APP or a distributed DAPP. For example, the application mall and the community governance website that are built in this ecosystem are centralized. They use IPFS, Internet, Internet of Things, etc. to connect to the blockchain service nodes to use the various functions of the blockchain, enjoy the blockchain completely decentralized, open and transparent, data can not be tampered with, traceable, low maintenance costs, all Various advantages such as joint governance.

The blockchain of all walks of life in this ecosystem, they share users, share markets, share technologies, share application solutions, and they are symbiotic and co-prosperous.

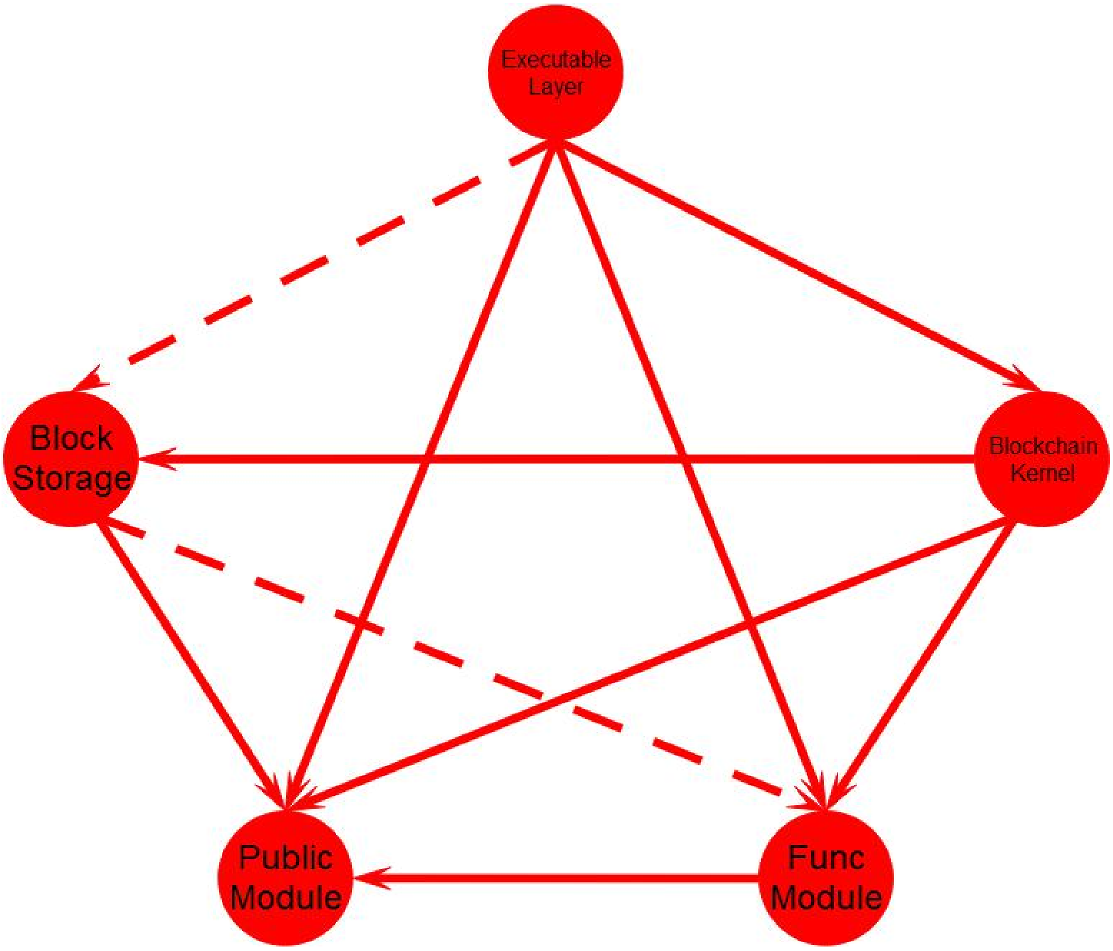


This is the core technical architecture that carries the blockchains of all walks of life. This architecture is divided into four levels: executable layer, sub-chain (public chain, alliance chain, private chain), main chain, and block storage layer.

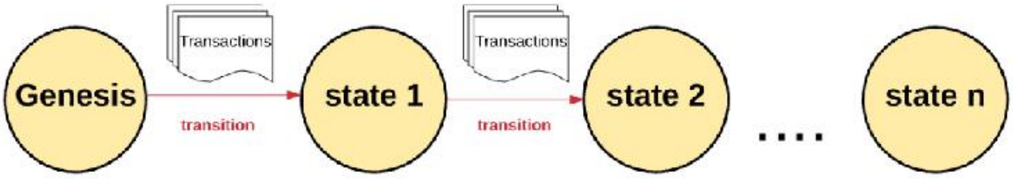


4.2.5.2 Pentagram architecture

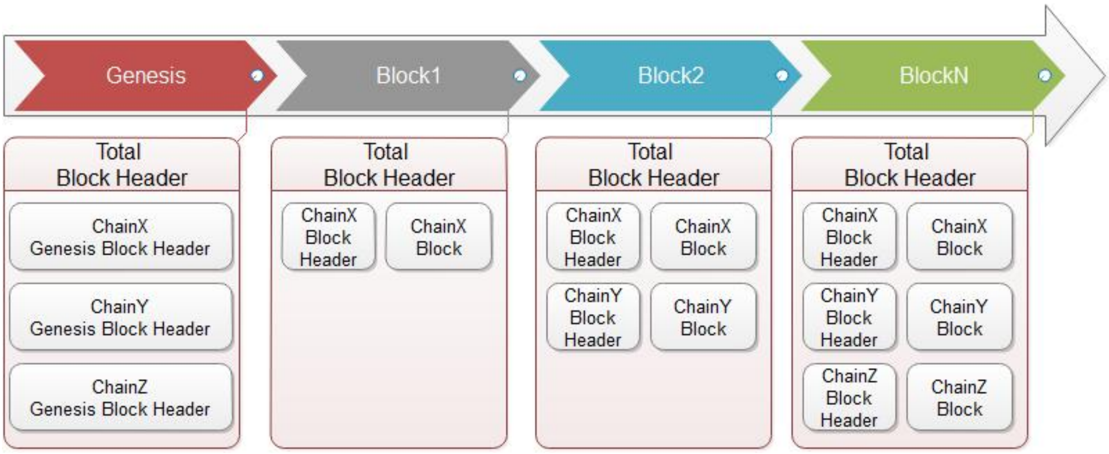
Each blockchain can also adopt a five-pointed star structure, as shown in the following figure, divided into an executable layer, a blockchain kernel layer, a block storage layer, a function module layer, and a public bottom layer.



4.2.5.3 Database State Diagram



4.2.5.4 Block storage map

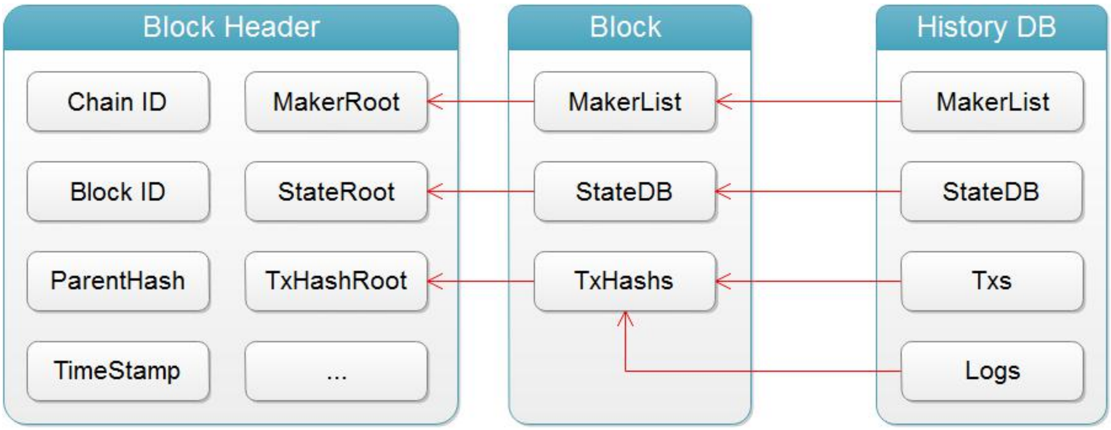


4.2.5.5 Segregated Witness

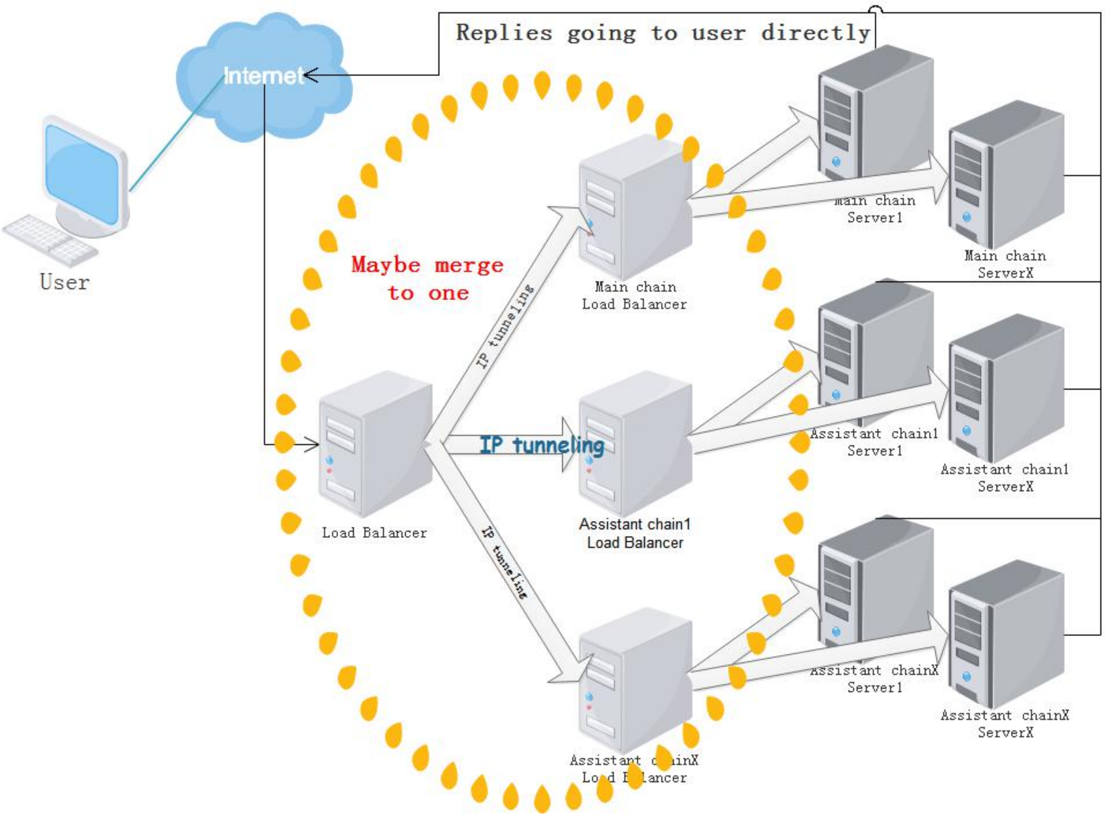
The concept of Segregated Witness (SegWit) is that transaction signatures are not relevant after a transaction is immutably included in the blockchain. Once it is immutable the signature data can be pruned and everyone else can still derive the current state. Since signatures represent a large percentage of most transactions, SegWit represents a significant savings in disk usage and syncing time.

The same concept can also be used throughout the block store: once the transaction is irreversibly recorded on the blockchain, the block only needs to permanently store the database state and the transaction hash that caused the state transition, while the transaction details and transaction log will be pressed. The retention time of the service node configuration is temporarily stored. All database status, transaction details, and transaction logs are stored in the data node's historical database.

It can also be understood that there are two parallel blockchains in each chain, one is the state chain that stores the latest state of the database, and the other is the historical chain that stores all the data. The history chain exists only in the data nodes. All service nodes need to synchronize the state chain and do not need to synchronize the history chain unless he requests synchronization.



4.2.5.6 Network topology



4.3 Business Ecology

This ecology insists on doing business, and the goal is to change the lifestyle of every user in the world. The business ecosystem between the various chains of the ecosystem is interdependent, and many businesses are coordinated by multiple chains. We are responsible for extending the entire ecosystem to the world, so the chain transaction fees for each chain (similar to Bitcoin's miners' fees) are transferred to the contribution fund.

4.3.1 Main chain

Manage accounts, digital currencies, smart contracts, interactions with the secondary chain, and more. Smart contracts can only be published to the main chain, but can interact with the secondary chain.

4.3.2 Payment chain

The payment chain is an organic combination of central banks, banks, payment companies, exchanges, and currency exchange companies. Support for legal currency - legal currency, legal currency - digital currency, digital currency - digital currency transaction, transfer (same currency), remittance (cross-currency), currency exchange (same account), small quick payment, credit prepayment, etc. Features.

4.3.3 Credit chain

Track the credit value of your account. Transactions are divided into three categories: rewards, deductions, and regular self-growth.

4.3.4 Certification chain

The legal person status of the certification account is based on the degree of cooperation with each country, and the household registration or KYC audit is adopted. The chain will use cryptographic algorithms and zero-knowledge proof algorithms to protect all privacy.

4.3.5 Notary chain

Prove the authenticity and legitimacy of various forms of affairs such as acts, facts, contracts, and wills. The chain will use cryptographic algorithms and zero-knowledge proof algorithms to protect all privacy.

4.3.6 Industry chain

A collection of industry chains from all walks of life.

4.3.7 Small quick payment (mobile payment)

The payment chain launches small, fast payments across every corner of the world, supporting a variety of legal and digital currency transactions.

4.3.8 Patronus and guardian Elf

Launching the patron saint and guardian elves on the credit chain, his savvy performance increases the credit growth factor, and his basic attributes are superimposed on the owner's credit value.

The patron saint needs the main chain assistance, all or part of the sub-chain coordination (only the public chain), because some of his immortal methods are applicable to all chains. The magic of the guardian elf applies only to the credit chain. An account can have multiple patrons and guardian elves. Their fairy and magic effects can be superimposed, but the savvy and basic attributes cannot be superimposed. Subsequent integration with the credit prepayment function of the payment chain. As for the UI effect display and other functions, tentatively combined with the wallet, it is also possible to develop an application specifically.

4.3.8.1 Patronus

The patron saint is unique in the entire ecosystem and consists of mythical figures and historical celebrities. Each patron saint has its own unique fairy law. The basic attribute is to be determined, and the scope of savvy is 60-100, that is, the credit growth factor is increased by 60-100 times. The rationality of the related items, the nature of the blockchain, the harm to the user's interests, the ethics and morality, the respect for the celebrities, the need to associate with the deputy chain, etc., the patron saint must meet these prescribed elements before they can be launched, and each element cannot be forced to join. The patron saint is only acquired by the auction, and there is no marriage function, but God can create everything, and the guardian elves created by it are the first generation. If it is entirely the patron saint of the design of the entry chain, 80% of the proceeds after the auction belong to it.

If the question mark in the table below cannot be resolved, then the ecology has only two patrons.

Patron	S	**Savvy**	**Fairy**	**Impact chain**	**Fairy Feature**	**Rationality statement**
Zhao Zilong	M	81	七进七出	All block chain	1. Free of all transaction fees; 2. The transaction is processed immediately; 3.There is no limit on the number of transactions in a period of time;	1. Does not harm the interests of users; 2. Many chains have mechanisms for high miners to be processed immediately; 3. Some chains adopt this mechanism only to prevent DDOS attacks; In summary, the required elements can be met.
Zhuge Liang	M	95	草船借箭	Main chain, Payment chain	1. Unsecured and interest, the maximum amount of money can be 10 million, with a term of 1 year; 2. After all the returns, you can	Similar to the securities industry's margin financing and securities lending, guaranteed by

					re-melt the coins; 3. The patron saint cannot be sold during the coin period; 4.If the local currency cannot be returned after expiration, the account will be frozen and the patron saint will be recycled and re-auctioned;	the security fund, without damaging the interests of users; In summary, the required elements can be met.
Luban	M	89	?	? 建筑链	?	?
Nüwa	F	96	?	?	?	?
Einstein	M	95	?	?	?	?
Cupid	M	79	? 爱情之箭	? 爱情链 婚介链	?	?
Athena	F	85	?	? 艺术链 公证链	?	?
God	M	100	? 上帝之手	? 证券链	?	?
?	?		?	?	?	?

4.3.8.2 Guardian Elf

The guardian elves are composed of elves, mammals (such as cats, dogs, pandas, dragons, phoenixes, etc.), each with different magic, such as dragons and phoenixes. Magic only affects the credit chain, and it is not necessarily effective every time after the exhibition. . The basic attributes are to be determined, and the range of savvy is 2 to 20 (randomly generated at birth). The same kind of opposite sex can be married and born. Access is available through auctions, partial initial account giving, and reproduction and patron saint creation. Each species only has an initial number of 1000 (provisional) for each male and female.

4.4 Digital currency

The main chain and all public chains unanimously issue the same digital currency, which can be circulated in all chains of the ecosystem, including the main chain, the public chain, the alliance, and the private chain. Each public chain defines a total of 210 million digital currencies, which are used to reward nodes that contribute when generating blocks. The public chain does not allow pre-issuance of digital currency. Only the main chain can pre-issue 1 billion coins for the development of the main chain and public welfare public chain, and to maintain the sustainable development of this ecosystem.

The public chain can pre-issue its own tokens, and the alliance chain and private chain can also issue their own tokens (pre-release or block rewards), but these tokens can only be circulated in their own chains. This means that there is only one digital currency and N tokens in the entire ecosystem.

In this ecosystem, this digital currency and any of the N tokens can be traded freely. The ecological public payment chain can carry out legal currency transactions, legal currency-digital currency transactions, currency transactions, and no external exchanges are required. We will insist that digital currencies are not external to the exchange (not active, passive to retain rights), and prohibit any foreign exchange on the token, the purpose is to limit the token for pure ICO purposes.

To be a stable digital currency in a global circulation, you must have the following elements:

- ➢ The circulation plate should be appropriate, not too big or too small;
- ➢ The price should not be too high, and should be relatively flat with the price;
- ➢ The price must remain relatively stable for a period of time and cannot rise or fall sharply;
- ➢ Need good liquidity, and promote and operate on a global scale;

Assuming that the ecology has one main chain, N public chains, M alliances or private chains, then the total ecological digital currency Y (unit: billion) is:

$$Y = 10 + 2.1 * (1 + N)$$

The issue price of digital currency is **1.688** yuan (CNY), and the planned use of the main chain of **1 billion** coins is:

4.4.1 Security fund

The total amount is 600 million coins. This is a guarantee and a smooth fund. This portion of the currency will be placed in a separate account so that each transaction is open, transparent and traceable.

- ➢ Full or partial guarantee for the business of this ecology, the total amount does not exceed 300 million coins.

- When the price of the currency rises or falls sharply, the smooth fund will be used to stabilize the currency price.

4.4.2 Contribution fund

The initial amount is 200 million coins, which are kept in the creation account and disclose all expenditures in the community. Subsequent auctions of premium account names, auction patrons and guardian elves, transaction fees, etc. will be transferred to the Fund.

The Fund is used to reward groups or individuals who contribute to the ecology today or in the future. Such as cryptography algorithms, zero-knowledge proof algorithms, compression algorithms, databases, communications, Boost, serialization, etc., or EIP and bugs, as well as the entire founding team, as well as the best operating chain and applications, "Luck Candidate producer node for the difference.

This is a sustainable reward mechanism, similar to the dividends of listed companies. In the first half of the year, the first dividend will be launched after the main online line. This part of the reward program is further refined.

4.4.3 Give away rewards

The total amount is 100 million coins. After delivery, you must pay attention to the balance of the smart contract before the shoot.

The ecosystem publicly auctioned 20,000 initial accounts in the form of smart contracts, with a reserve price of 5 ETH and a time of 187 days. I bought 3,500 coins in the first 97 days, and I donated 2,000 coins in the rest of the time. The first 37 days to buy also added a guardian elf. For the part with an auction price of more than 5 ETH, an additional 800 coins will be given for each ETH. That is, if you buy with 5 ETH in the first month, you will get an initial account and a guardian elf and 3,500 coins; if you buy with 8.9 ETH in the first month, you will get an initial account and a guardian elf and 5,900 coins (3500 + 800 * 3). After the contract is over, the highest auction price (only one, the same price, the priority of the auction time), plus a patron.

The initial account has exclusive rights to select the account's premium name (length 2 to 10). If the name is the same, it will be executed according to the principle of high auction price and early purchase time. The winners need to be re-selected. These accounts are the initial accounts that have been created when the main online line is created. Compare the auction price of the EOS account, which is equivalent to white delivery. Please see the "Accounts" chapter for more information.

The initial account is the goal pursued by premium account name enthusiasts, while the patron saint is a game of wealth free, and does not recommend user participation without material foundation. An ETH account can only take one initial account.

Smart contract：

https://etherscan.io/address/0x54850c1601826b3958b25bd995efc26a52044c0a

4.4.4 Stationed chain reward

The total amount is 50 million coins. The top 20 public chains, each chain can apply for a reward of 1 million to 10 million coins.

The reward amount is evaluated according to the amount of users, the influence of the chain, and the contribution to the ecology.

This ecology welcomes the existing lone chain of all walks of life to join together to create a symbiotic and coherent blockchain ecosystem.

4.4.5 Stationed APP reward

The total amount is 48 million yuan. The top 500 APP or DAPP that are stationed in the app store, whether centralized or decentralized, can be applied for a reward of 10,000 to 2 million coins, either on the PC side or on the mobile side.

The reward amount is assessed according to the amount of users, the influence of the application, and the contribution to the ecology.

Many existing centralized applications, such as WeChat, Taobao, Jingdong, Vibrato, Jedi Survival, King Glory, etc., as long as access to the ecological backbone, certification chain, credit chain, notary chain, payment chain or any other Or multiple chains can participate in this ecosystem.

4.4.6 Airdrop

The total amount is 2 million coins.

4.5 Ecological governance

Each chain should have its own community to manage the affairs of the chain. The community of this ecology only manages the rules and codes of conduct that all chains of this ecology need to abide, and the main chain affairs. We do not interfere with each chain's own affairs.

This ecological wallet will bring its own voting function, vote according to the proportion of the currency, and all the people will decide all matters.

The main chain has the following transactions:

4.5.1 Freeze and unfreeze accounts

Sometimes a smart contract behaves abnormally or unpredictably and cannot be executed as expected; an application or account may find a vulnerability that can be exploited. When these problems inevitably occur, the Ecology has the right to freeze these accounts. When these accounts return to normal, they can be thawed.

4.5.2 Change account legal person key

The legal person key can be replaced as long as it is certified by the legal person in the certification chain.

4.5.3 Organize EIP voting

EIP voting is initiated regularly in the community, and users can also vote in the wallet client.

4.5.4 Stationed chain resource allocation

Allocate and publish resources such as the ID of the inbound chain in the community.

4.5.5 Cash contribution award

Collect a list of contributions in the community, regularly redeem the contribution awards, and post the rewards in the community column.

4.5.6 Emergency change

Urgent changes to be made when fixing a serious bug or damaging a user's security breach.

4.6 Module management

4.6.1 Module release

Modules for the entire ecosystem require a signature to be released.

4.6.2 Module check

The program can automatically verify that each module's signature is correct and verify that it is legal and tampered with.

4.6.3 Module update

Divided into soft updates and hard updates.

4.7 Node classification

4.7.1 Classified by performance

4.7.1.1 Main node

This kind of node can automatically deploy all public chains; it requires very large CPU computing power, memory, storage space, bandwidth and other resources. It is recommended to use IaaS to build.

4.7.1.2 Trunk node

Nodes with partial chain deployment (including the main chain) are deployed. Depending on the number of deployment chains, it is decided to choose IaaS or a normal server to build.

4.7.1.3 Branch node

Only a single sub-chain node (including the main chain) is deployed. This kind of node is usually built by the chain itself. It only serves the main chain and can be used by ordinary servers. This node is mostly a node of a federation chain or a private chain.

4.7.2 Classified by function

4.7.2.1 Query node

Check the command format and the server that processes the query command. Such a node is usually an old server that needs to be eliminated, or a temporary server built by a company or an individual.

4.7.2.2 Trading node

A server that checks command formats, processes query commands, processes transaction commands, consensus transactions, and generates blocks. Such nodes need to bind accounts to receive block rewards. Corresponds to candidate producers and producers in the list in Section 6.2.

4.7.2.3 Data node

A server that stores historical data such as database status, transaction data (transaction details), transaction logs, and other analytical data. There are only a small number of data nodes. All data nodes will form a cluster, recap all data, analyze the correctness of the data, and once the abnormal data is found, all data node consensus will be submitted. Once the data is confirmed abnormal, the node submitting the data will be processed.

5 Sharding

The low efficiency of the ecological solution consensus is to introduce fragmentation technology into the consensus algorithm to improve the scalability of all blockchains and achieve high throughput. The ecology will be divided into 16 (provisional) areas, with the account as the target, then all transactions will be divided into two areas: the same area transaction and the cross-region transaction; the same area transaction will be based on the consensus results of each district. Will be packaged immediately; cross-zone trading requires a consensus of all areas, there will be a certain delay. The use of fragmentation technology not only improves the efficiency of consensus, but also reduces the data redundancy of transmission (many data will no longer be transmitted by broadcast), TPS can at least increase by several times or even more than the existing blockchain. Hundreds of thousands of times (and the parabolic relationship between the number of sub-areas), the ecological TPS target is about 30,000, which can fully support the needs of large-scale commercialization. You know, VISA has more than 20,000 TPS.

There are three types of fragmentation schemes for consensus algorithms:

5.1 Sharding by region

Accounts and service nodes are fragmented by region (or by time zone or other). This algorithm is simple to implement, but has a little centralization. Please refer to Section 6.1.1 for details.

5.2 Semi-random sharding by algorithm

One of the account or service nodes is fragmented by region (or by time zone or other), and the other is randomly fragmented by the consensus algorithm, such as account name hash fragmentation, node IP hash fragmentation. This algorithm is relatively compromised. Please refer to Section 6.1.2 for details.

5.3 Full random sharding by algorithm

Both the account and the service node are randomly fragmented by the consensus algorithm. This algorithm is the most complicated. Please refer to Section 6.1.3 for details.

6 Consensus algorithm

This ecology adopts the consensus mechanism of X-sharding Y-consensus (X, Y = [1, N), which is first introduced in 1 time and 2 times consensus). This is a consensus algorithm based on the complete decentralization of the fragmentation technique, namely the Byzantine Fault Tolerance-Proof of Contribution with Sharding (BFT-PCS). According to this algorithm, any node can become a block producer as long as certain capability requirements are met, and the software version, transaction processing speed, and transaction processing total are hard indicators. The proof of contribution is based on the proof of the workload. The nodes that have processed 100,000 transactions have been processed, and the nodes that have processed 10 transactions are more reliable. The consensus is not based on the order of the transactions, but on the first-to-block.

6.1 Algorithm implementation

6.1.1 BFT-PCS(A)

The account and service nodes of this algorithm have been divided into 16 (provisional) areas by region. The steps are as follows:

1. Evaluate the capability index of the node according to the total transaction processing volume, network speed, CPU, memory, storage space, etc.

2. When the node whose capability index reaches the predetermined threshold synchronizes the information that must be synchronized, it can be added to the candidate producer list; if it is not synchronized due to dropped or other reasons, the candidate producer will be temporarily removed from list.

3. The first producer list for each chain is generated by the node bound by the

creation account of the genesis, and the subsequent generation is randomly generated by the fourth production node (16 * 1⁄4) of the previous round.

4. The producer list is generated by:

The first step extracts 4 (provisional) nodes from the list of candidate producers in each of the 16 regions; if the number of nodes in a certain region is 0, the nodes are not extracted, and the transactions in the region are processed in the cross-region; if only 1 Nodes are not extracted from the replacement node; unless the number of nodes is insufficient, they are not allowed to extract themselves;

The second step sets the 16 nodes extracted from each slice for the first time to the predetermined production nodes of each slice, and the nodes extracted later are set as substitute production nodes;

The third step broadcasts the producer list to the entire network.

5. In the production time period of the 8th production node (16 * 1⁄2), check whether there is cheating in the next round of producer list. If cheating, add the node that generated the list to the blacklist; and the production node Regenerate; if legal, all nodes need to store the next round of producer lists;

6.When there is a scheduled production node in the producer list that is not working properly, it will be immediately added by the replacement node. If the replacement node is not working properly, the area will be skipped and the next block node will continue to produce the block;

7.According to the fixed order of the producer list, 4 (provisional) blocks are successively produced by the production node, and one block is generated every second; with the originating account as the target, the transaction in which the originating account is not the area will be forwarded to the same. Service node processing in the area; in a block consensus process, first agree on the same area transaction, and then consensus across the area transaction. The nodes of each tile (or only the 3 substitute nodes are reserved by the tile 1) only agree on the same zone transaction of the own zone; then only 16 predetermined producers agree on the cross-zone transaction. The transactions in the same area of the 16 scheduled producers are immediately packaged into the block, while the cross-segment transactions require them to be packaged into the block after the consensus is passed; most of the time for a block is used for the consensus across the block. Trading, but the volume of transactions reached consensus is far less than that of the same area;

8. The total time of each round is 64 seconds (16 * 4). After the end of each round, all the reward coins generated by this round are equally distributed to all nodes in the producer list by the last production node of this round.

9. Start a new round of consensus according to the next round of producers

generated in step 3.

6.1.2 BFT-PCS(B)

Assuming that the service node has been fragmented and the account is fragmented by an algorithm, the algorithm steps are similar to A and are omitted here.

Assuming the account has been fragmented, the service node is fragmented by the algorithm. The steps are as follows:

1、Same with A；

2、Same with A；

3、Same with A；

4、The producer list is generated by:

In the first step, the nodes in the candidate producer list are randomly divided into 16 (provisional) tiles; if the number of nodes is insufficient, how many nodes are divided into blocks, and there is one node segment corresponding to multiple account segments. ;

The second step extracts four (provisional) nodes from the list of candidate producers in each of the 16 regions; if there is only one node, the substitute nodes are not extracted; unless the number of nodes is insufficient, it is not allowed to extract itself;

The third step sets the 16 nodes extracted from each slice for the first time to the predetermined production nodes of each slice, and the nodes extracted later are set as substitute production nodes.

The fourth step broadcasts the fragmentation results and producer lists of all nodes to the entire network.

5、In the production time period of the 8th production node (16 * 1⁄2), check whether there is cheating in the next round of producer list. If cheating, add the node that generated the list to the blacklist; and regenerate it by the production node. ; if legal, all nodes need to store the next round of fragmentation results and producer list;

6、Same with A；

7、Same with A；

8、Same with A；

9、Start a new round of consensus according to the next round of fragmentation results and producer list generated in step 3;

6.1.3 BFT-PCS(C)

The algorithm account and the service node are all fragmented by the algorithm, such as hashing according to the account name and node IP hashing. The steps are as follows:

1、Same with A；

2、Same with A；

3、Same with A；

4、The producer list is generated by:

The first step is the same as B;

The second step is the same as B;

The third step is the same as B;

The fourth step randomly divides all accounts into X areas (X = node fragments);

The fifth step broadcasts the fragmentation results and producer lists of all accounts and nodes to the entire network.

5、Same with B；

6、Same with A；

7、Same with A；

8、Same with A；

9、Same with B；

6.2 Algorithm Features

The node function rights of this algorithm are classified as follows:

Role		Check command Query command	Trade	Consensus	Production block	Reward coin
Query node		√	✖	✖	✖	✖
Candidate producer		√	√	✖	✖	✖
Producer	Book	√	√	√	√	√
	Substitute	√	√	√	Unknown	√

The algorithm has extremely high randomness and unknownness, which is completely decentralized and eliminates the possibility of cheating. If a node is identified as untrustworthy or cheater by the entire network, it will be added to the blacklist, and the node will no longer be added to the candidate producer list. The account bound to this node will also be punished accordingly.

In theory, this ecological blockchain does not experience any forks, because in the block production process, producers are cooperative rather than competitive, and producers are traceable. If a fork (non-hard fork) occurs, it means that this is a deliberately created fork, and the consensus will automatically trace the source and switch to the legal chain.

The Byzantine fault tolerance mechanism is added to the consensus algorithm. Based on multiple signatures, by allowing all predetermined producers to sign blocks, once 11 (by 16 tiles) producers sign a block, the block is considered irreversible and the irreversible consensus can be within 1 second. Achieved. If a Byzantine producer signs two blocks with the same timestamp or the same block height, the algorithm automatically adds the node to the blacklist.

6.3 Transaction confirmation

In this consensus algorithm, the asynchronous Byzantine fault-tolerant algorithm (aBFT) will be added to achieve faster irreversibility.

Due to the inconsistent speed of the transaction writing block, the same piece of the transaction can be irreversibly confirmed in 1 second, and the cross-sliced transaction takes 1~4 seconds to obtain irreversible confirmation. But this is acceptable to the user.

7 Accounts

The account types are divided into five types: government units, organizations, companies, individuals, and initial accounts. The readable name of the account is 2 to 10 characters long and consists of letters and numbers. Accounts are the only credentials that pass through the entire ecosystem.

The account name is freely chosen by the creator. Government, organizations, and company accounts must be certified by the certification chain to register. These three types all come with suffixes. Personal accounts are not mandatory, but there is no way to modify the corporate key and PIN after losing the key. The freely created account can only be 10 characters in length. Other lengths can only be obtained from the auction. The account obtained after the online auction does not belong to the initial account; the initial account is a special personal account. These accounts are all veteran and can only be used. Auctioned in the smart contract at the crowdfunding stage.

- Government is suffixed with .gov: china.gov，usa.gov
- Organization is suffixed with .org: abc.org
- Company is suffixed with .cl: google.cl，apple.cl，icbc.cl
- Ordinary personal account: oneperson9，abcdefg123，1234567890
- Initial account: games，love，god，baby，money，coin

7.1 Actions and Handlers

Each account can send structured Actions to other accounts and may define scripts to handle Actions when they are received. System gives each account its own private database which can only be accessed by its own action handlers. Action handling scripts can also send Actions to other accounts. The combination of Actions and automated action handlers is how system defines smart contracts.

To support parallel execution, each account can also define any number of scopes within their database. The block producers will schedule transaction in such a way that there is no conflict over memory access to scopes and therefore they can be executed in parallel.

7.2 Role Based Permission Management

In an account, there can be up to five levels of rights management. The five levels of roles are legal person, management level, usage level, contract level, and onlooker level (unexecutable transactions, examples are binding service nodes). The system provides a custom privilege management system that provides fine-grained, high-level control of accounts and determines what each role can do and when.

It is critical that authentication and permission management be standardized and separated from the business logic of the application. This enables tools to be developed to manage permissions in a general-purpose manner and also provide significant opportunities for performance optimization.

Every account may be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical authority structure that reflects how permissions are organized in reality and makes multi-user control over accounts easier than ever. Multi-user control is the single biggest contributor to security, and, when used properly, it can greatly reduce the risk of theft due to hacking.

7.2.1 Permission Mapping

Allow each account to define a mapping between other accounts and their own account roles. For example, a company account can map an employee's account to a corresponding role. Through this mapping, these employees can be used as company account users, using the company account to allocate their own funds, but they still use their own key to sign.

7.2.2 Parallel Evaluation of Permissions

The permission evaluation process is "read-only" and changes to permissions made by transactions do not take effect until the end of a block. This means that all keys and permission evaluation for all transactions can be executed in parallel. Furthermore, this means that a rapid validation of permission is possible without starting costly application logic that would have to be rolled back. Lastly, it means that transaction permissions can be evaluated as pending transactions are received and do not need to be re-evaluated as they are applied.

All things considered, permission verification represents a significant percentage of the computation required to validate transactions. Making this a read-only and trivially parallelizable process enables a dramatic increase in performance.

When replaying the blockchain to regenerate the deterministic state from the log of Actions there is no need to evaluate the permissions again. The fact that a transaction is included in a known good block is sufficient to skip this step. This dramatically reduces the computational load associated with replaying an ever growing blockchain.

7.3 Double key protection

This ecosystem will use another elliptic curve algorithm. In addition to the private key, the user password PIN (numbers 4-12) will be added. A special mechanism will be used to generate the PIN Block from the PIN calculation, and the PIN Block will participate in the signature and verification. The calculation of the sign, so that only the private key and PIN are correct, the signature can be verified and the transaction can be successful.

The user only needs to store the private key and the PIN separately, or the PIN is not stored at all, and only remains in the memory, which greatly enhances the security. Even if someone steals your private key, you can't steal your assets.

The private key and PIN are equally important and must be kept by the user.

7.4 Stolen account recovery

Provides users with a way to restore their account control when the account is stolen, provided they are certified by the certification chain.

- The private key cannot be retrieved. After the private key is stolen or lost, the legal person's public key can be reset only after passing the legal person authentication. Otherwise, the account can only be discarded.
- The PIN can be reset according to the old PIN (similar to the bank modification password). If you forget the PIN, you need to pass the legal person authentication to reset.

8 Scripts and Virtual Machines

The details of the scripting language and virtual machine are implementation-specific details that are mostly independent of the technical design. Any language or virtual machine can be integrated with the API, which has sufficient performance and determinism and correct sandboxing.

8.1 Schema Defined Action

All Actions sent between accounts are defined by a schema which is part of the blockchain consensus state. This schema allows seamless conversion between binary and JSON representation of the Actions.

8.2 Schema Defined Database

Database state is also defined using a similar schema. This ensures that all data stored by all applications is in a format that can be interpreted as human readable JSON but stored and manipulated with the efficiency of binary.

8.3 Generic Multi Index Database API

Developing smart contracts requires a defined database schema to track, store, and find data. Developers commonly need the same data sorted or indexed by multiple fields and to maintain consistency among all the indices.

8.4 Separating Authentication from Application

To maximize parallelization opportunities and minimize the computational debt associated with regenerating application state from the transaction log, separates validation logic into three sections:

1.Validating that an Action is internally consistent;

2.Validating that all preconditions are valid; and

3.Modifying the application state.

Validating the internal consistency of a Action is read-only and requires no access to blockchain state. This means that it can be performed with maximum parallelism. Validating preconditions, such as required balance, is read-only and therefore can also benefit from parallelism. Only modification of application state requires write access and must be processed sequentially for each application.

Authentication is the read-only process of verifying that an Action can be applied. Application is actually doing the work. In real time both calculations are required to be performed, however once a transaction is included in the blockchain it is no longer necessary to perform the authentication operations.

8.5 Code is separated from the instance

Smart contracts are developed in a modular way. An identical smart contract module stores only one copy in the block. Separating the code of the smart contract from the execution instance helps to improve the reuse rate of the code and also reduces the storage space of the block.

The developer uploads the smart contract code to the application store for the user to browse and publish the compiled module to the block. When the user uses the module, they need to pay the developer's preset fees in one lump sum. Because the cost of publishing and direct use is similar, and the release needs to be reviewed, it protects both the developer's rights and the existing modules.

8.6 WASM

WASM is the latest standard for building a high-performance Web that can be clearly defined and sandboxed with a small amount of adaptation. It has been widely supported by the industry, and currently mainstream browsers already support WASM.

This ecosystem will use WASM to build smart contracts with a development language of C++.

We will provide intelligent contract interface modules and adaptation modules based on the C2I architecture, allowing APP/DAPP developed in any language to interact directly with smart contracts.

9 Communicate with the blockchain node

9.1 Transaction delay

When communicating with the blockchain, the application must determine 100% that the transaction is irreversible and then consider the result as the final result.

9.2 Proof of integrity

At the bottom of the blockchain, each account has its own serial number. Adding the serial number of the account in the command can prove that all the instructions of the account have been processed. According to the user's operating frequency, the transactions are processed in order.