111111111111

KOK certificate

KOK Block Chain Pass Card

Block-based Belt and Road ASEAN
Settlement solution

table of Contents

Chapter 1 Background of the KOK Pass

With the rapid development of the Internet era, more and more science and technology have emerged, but the most popular blockchain technology is the blockchain technology, which is only used as the underlying technology of Bitcoin to record the reasonable operation of Bitcoin. But as time went on, people discovered the stability advantage of the blockchain.

Development prospects of blockchain

1. Features

Decentralization: Damage or loss of any node will not affect the operation of the entire system.

Reliability and non-destructive modification: Destroying blockchain systems requires attacking more than 51% of nodes.

De-trust: Participating in data exchange between each node in the whole system does not need to trust each other. The operating rules of the whole system are open and transparent.

Collective maintenance: The data blocks in the system are maintained by all nodes with maintenance functions in the whole system. These nodes with maintenance functions are distributed and can be participated by anyone.

2. Development prospects

According to the blockchain utility roadmap released by McKinsey:

2014 to 2016 is the blockchain technology assessment phase;

The concept verification phase will be entered from 2016 to 2018;

From 2017 to 2020, blockchain infrastructure will enter the formation phase, develop a comprehensive user interface, leverage API interfaces for product development, achieve less manpower, and reduce costs by sharing infrastructure;

After 2021, it will truly enter the stage of asset diffusion, and blockchain technology will be fully applied.

In two reports last September, IBM pointed out that 14% of banks surveyed and financial market institutions surveyed plan to fully implement commercial blockchain solutions in 2017. IBM believes that the large-scale adoption of blockchain technology is not far away, and nearly 65% of banks are expected to adopt blockchain solutions in the next three years.

3. Policy support

In recent years, government policies and financial support for blockchains are gradually increasing.

The ASEAN "One Belt, One Road" is an important strategic measure for China to coordinate domestic economic development and deepen its opening up. Southeast Asia is the priority development side of China's neighboring diplomacy.

As one of the important areas covered by the “Belt and Road”, ASEAN is an important strategic partner of China and an important participant in the construction of the “Belt and Road”.

The application of blockchain technology in cross-border payment can be divided into two main categories:

One is to use digital currency as a lubricant for currency exchange. The use of private digital currency as a medium of exchange for different currencies in cross-border payments, in theory, enables seamless and fast exchange between any

two currencies.

The second is to regard blockchain technology as an interface technology between payment institutions and commercial banks. Multi-party cross-border remittances transmit remittance messages to each participant through blockchain technology, thereby achieving multi-party collaborative information processing, parallelizing serial processing between the original organizations, and improving information transmission and processing efficiency.

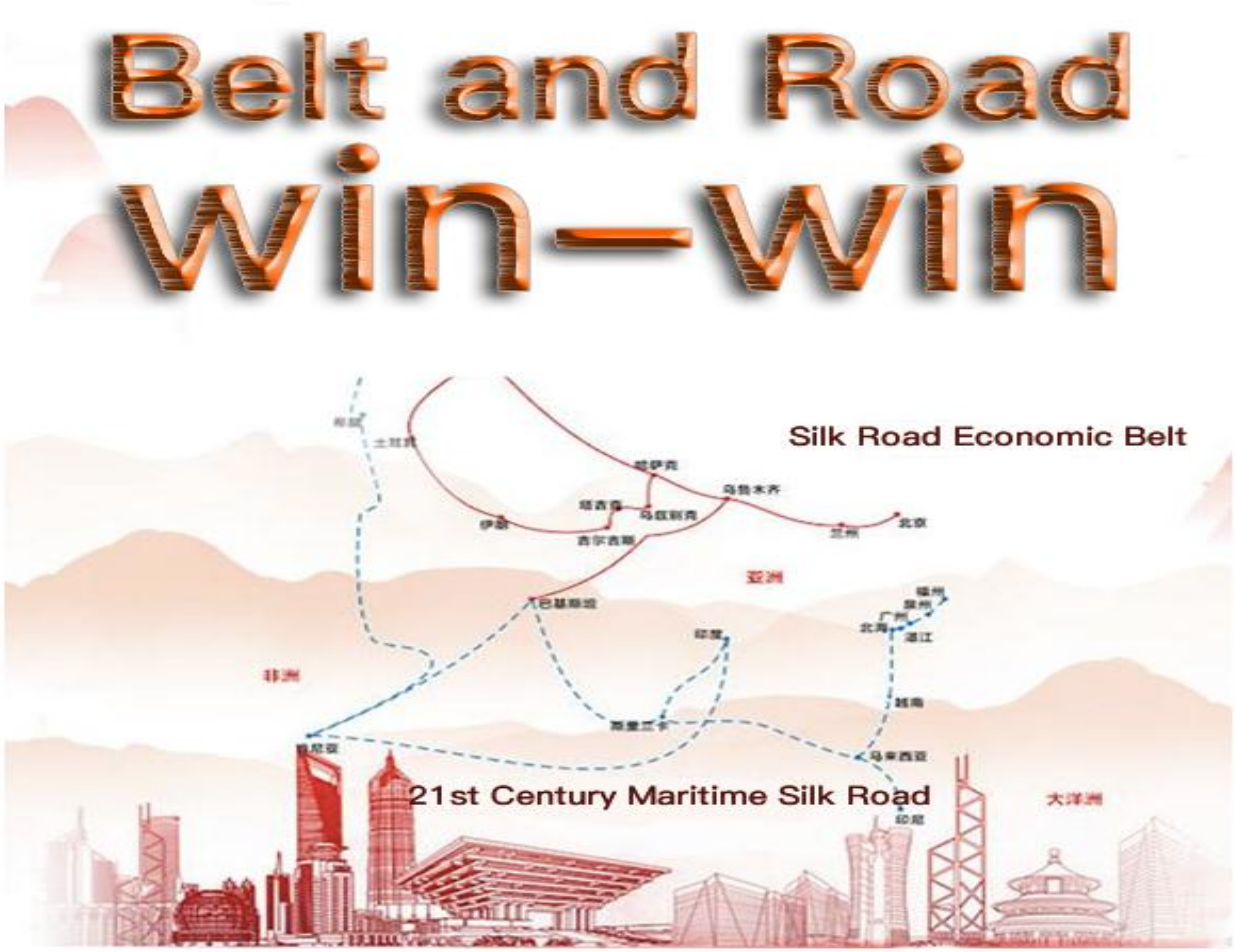
In 2008, after Satoshi Nakamoto proposed the concept of blockchain, the world started a blockchain technology trend with decentralization, rebuilding trust mechanism and value communication. At the same time, the digital currency market with blockchain as the underlying technology has ushered in the development of spurt in the past ten years. Today, the global digital currency market has reached more than 1,500 digital currencies, a market size of $300 billion, and more than 500 digital currency trading platforms.

Unfortunately, most traditional exchanges have highly centralized attributes, which is a serious violation of the core nature of the blockchain – decentralization. More critically, most exchanges, as vested interests, have opaque assets, unfair distribution of interests, weak underlying infrastructure, backward security protection techniques, chaotic currency rules, and even black-box operations. In order to promote the development of the global blockchain industry, the market urgently needs an innovative, democratic, transparent, equal, free and secure trading environment to cope with the escalation of the blockchain industry and promote the formation of a global exchange. A more benign competitive landscape. History will not forget the highlights of the blockchain industry, as well as the hope that the blockchain will bring to the global trust mechanism and the vision of redefining the world. Because of this, we have created a KOK Pass based on our deep understanding of the blockchain revolution and our key contribution to the global blockchain busine

Chapter 2 KOK Pass: One Belt and One Road Based on ASEAN

2.1 Belt and Road, based on ASEAN

The “Belt and Road” is an important strategic measure for China to coordinate domestic economic development and deepen its opening up. Southeast Asia is one of the priority development directions of China's neighboring diplomacy and one of the important areas covered by the “Belt and Road”. ASEAN is China's important strategic partner. An important participant in the construction of the “Belt and Road”. The “Belt and Road” has injected a new concept of “equality negotiation”, “mutual assistance and mutual construction” and “open sharing” for the development of China-ASEAN economic and trade relations, and established a new platform of “advantageous industry cooperation”, “diversified innovation” and “strategic docking”. The new mechanism of “decision and docking”, “market-oriented operation” and “cross-national connectivity”. At the same time, the promotion of the “Belt and Road” in Southeast Asia faces negative influences from factors such as the growth of nationalism within the ASEAN countries and the interference of extraterritorial powers.



List of countries along the Belt and Road

One. China, including Mongolia in East Asia, 10 countries in ASEAN: (Singapore, Malaysia, Indonesia, Myanmar, Thailand, Laos, Cambodia, Vietnam, Brunei and the Philippines), subtotal 12 countries

Two. 18 countries in West Asia (including Egypt in North Africa and Greece, Cyprus in Europe): (Iran, Iraq, Turkey, Syria, Jordan, Lebanon, Israel, Palestine, Saudi Arabia, Yemen, Oman, United Arab Emirates, Qatar, Kuwait, Bahrain, Greece, Cyprus and Egypt)

Three. Eight countries in South Asia: (India, Pakistan, Bangladesh, Afghanistan, Sri Lanka, Maldives, Nepal and Bhutan)

Four. 5 countries in Central Asia: (Kazakhstan, Uzbekistan, Turkmenistan, Tajikistan and Kyrgyzstan)

Fives. 7 countries of the Commonwealth of Independent States: (Russia, Ukraine, Belarus, Georgia, Azerbaijan, Armenia and Moldova)

Six. 16 countries in Central and Eastern Europe: (Poland, Lithuania, Estonia, Latvia, Czech Republic, Slovakia, Hungary, Slovenia, Croatia, Bosnia and Herzegovina, Montenegro, Serbia, Albania, Romania, Bulgaria and Macedonia)

2.2 Our Opportunities

Throughout the entire economic belt of the Belt and Road, it can be seen that the economic development of most countries and regions along the line is relatively lagging behind, the economic volume is low, the GDP is slightly lower, the inflation rate is higher, and the foreign exchange reserves are lower, which directly leads to The bulk trade between countries is subject to the government's foreign exchange reserves, which makes trading difficult, as shown in the following aspects:

1. The high inflation rate has led to the reluctance of other countries to accept their own currencies: most of the transnational barter trade projects are medium and large-scale projects or products, often with long trading cycles and large amounts of funds. However, most countries along the Belt and Road route have higher inflation rates, which will lead to a significant depreciation of the currency of the transaction when many projects or transactions have not been completed, directly affecting cross-border trade.

2. Low foreign exchange reserves, lack of hard currency, trade difficulties: For some relatively backward countries and regions, there is a lack of sufficient foreign exchange reserves of US dollars, euros or renminbi. Therefore, when it is necessary to purchase goods from other countries, other countries are more willing to accept payments in dollars, euros, etc., but these countries or regions lack sufficient foreign exchange reserves, which leads to trade difficulties.

According to the above main problems, we propose to solve the problem through barter trade, which can mainly serve the following aspects:

First, in order to ensure the supply of basic domestic living items and key projects, the government seeks barter settlement when there is a shortage of foreign exchange and loans are not available. For example, the government imports wheat, imports railway cars, and infrastructure construction. Under this circumstance, the government will take the initiative to help solve the trading problems of easy goods.

Second, under the foreign exchange management system, some entities have investment capabilities.

Through technological transformation of imported equipment, the project can obtain government approval, but the government is not responsible for resolving foreign exchange resources. These units have considerable local income each year and the project unit is willing to pay the local currency. Under this circumstance, it is necessary for the two parties to the transaction to solve the problem of the goods in good condition (the purchaser purchases the special products of the country with the local currency, and exchanges the equipment of the other with the special products).

Third, part of the transaction is paid in the form of local and foreign currency instalments. In the case of a transaction, the parties agree that the buyer will first settle 40% of the purchase price in US dollars, and the remaining part will implement the revenue sharing system and pay in local currency. In this case, the seller adjusts the exchange with other local companies, and only the units with branches in the poor countries can conduct trade. Some large-value transactions ultimately need to be conducted through barter trade.

At present, the barter trade form mainly focuses on the following aspects:

1. One-to-one bartering of the company: The two companies use bartering means to obtain each other's needs, w hile stocks last, not continuous barter;
2. Small-scale internal bartering: unified development of internal members by specialized bartering companies, un ified settlement, charging standards, internal free adjustment, each required;
3. E-commerce mode: The Internet company provides an online trading platform to collect membership fees. Eac h member unit is free to publish easy-to-change information, and free to do offline.transaction;
4. Inter-governmental bartering: The two governments have signed a bilateral barter agreement to exchange their own resources for other countries' products;
5. Coordination of civil organizations: The cooperation agreement is signed by the world's largest professional bar ter companies, which exchanges information of their members to achieve resource sharing and mutual benefit

There are several shortcomings in the above five types of barter trade:

1. There are few types of trading models, and often the products or services provided by enterprises are not ea sy to go out, and the products they need are not easy to come in;

2. There is no credit guarantee system, which is easy to cause the company to be deceived;

3. There is no unified global settlement system, lack of settlement tools and settlement standards, and it will no t be a long-term transaction;

4. Without uniform trading rules, companies cannot achieve transactions under fair and equitable conditions;

5. There is no unified management organization, and disputes cannot be settled;

6. No professionally recognized barter brokers;

7. There is no unified trading platform, barter information exchange is not smooth, and the transaction can not be supervised.

From the current forms and shortcomings of barter, it is necessary to establish a new barter trade model. A uni fied barter trade organization with members of the countries and regions along the Belt and Road, using the blockc hain digital currency settlement system as a settlement tool, using a dedicated international barter platform and a c entral city barter exchange as a trading platform to develop global unification Trading rules. KOK Pass is a barter tr ade platform built with blockchain technology, which can solve the above-mentioned related problems, and will also

solve the bottle diameter problem of modern barter trade development, providing unlimited business opportunities f or global barter trade, which is also the global barter. The inevitable trend of trade development.

2.3 Our goal

The KOK Pass Barter Trading Platform adopts a public chain barter trade network based on blockchain technology of commercial, political and civil use. It provides barter trade accounting, credit reporting, business relations through the barter trade blockchain. Comprehensive services of government regulation and multilateral trade integration. The barter trade service provided by KOK Pass provides access to production, supply and consumption links. Through the open account book of the blockchain, it can support multi-country, multi-enterprise and multi-user access, and support different terminal devices and different platforms to share barter. Book information, improve asset liquidity, and improve the economic strength of countries along the Belt and Road!

The KOK Pass Project is positioned as an international barter trade blockchain. It is supported by business resources and government channels owned by multiple countries and regions. It is mainly solved by blockchain technology:

1. Distributed accounting problem: In the international barter trade, the value of goods or projects is evaluated by international hard currency (such as US dollar and euro). When barter trade is carried out, the KOK pass blockchain is used for distributed accounting. Account, and through the trade to complete the cost of hedging.

2. Multilateral trading issues: Traditional barter trade tends to have something that is easy to come in, and some things are easy to go out. Through the KOK Pass asset path discovery function, up to 6 trading assets can be introduced for bartering, which greatly improves the reliability of the transaction.

3. Credit information: KOK Pass Barter trade chain united with the government departments and large industrial groups of the Belt and Road, building a barter trade chain, all transaction data is on the chain, through blockchain technology, once the transaction record can not be changed, the future All transactions are anchored to the trader's credit, and once breached, the consequences are very serious. At the same time, some large-scale trades also require the factoring company to do the corresponding services and the relevant banks to issue L/C letters of credit.

4. Settlement problem: The KOK Pass distributed account book has its own clearing and settlement function. It can be accounted for by the blockchain, and there is no need to carry out liquidation according to the traditional double-entry bookkeeping method. All transactions in the KOK Pass must be signed by the user's private key to confirm the bill, so all transactions of the KOK Pass are equivalent to settlement, which greatly reduces the settlement workload.

5. Trading rule problem: There are many uncertain factors in traditional barter, but through the KOK pass smart contract, the corresponding rules can be agreed before the transaction and written into the blockchain. When the conditions are met, they are automatically executed to avoid various types of disputes arising from the transaction process.

6. Regulatory issues: The goal of KOK Pass is to establish an honest barter trade environment. Governments and institutions are welcome to supervise the trading of assets on the chain. Through the KOK Pass, the barter trade chain can make the regulatory layer cost-effective and efficient. Regulate

barter trade compliance and meet the policy requirements of multiple countries.

Chapter III Basic Design Principles of KOK Pass

3.1 KOK Pass KOK is a public chain

The public blockchain refers to a consensus blockchain that anyone in the world can read and send transactions but can obtain valid confirmation. The public blockchain is the earliest blockchain and the most widely used (current) blockchain. The virtual digital currency of each bitcoins series is based on the public blockchain. There is only one currency in the world. Blockchain. The security of the public chain is responsible for maintenance in the form of a workload proof mechanism (pow) and a rights proof mechanism (pos). They exist in a combination of economic rewards and digital cryptographic verification, and follow the general principle: the economic rewards that each person can obtain are proportional to the contribution made to the consensus process. Often referred to as "complete decentralization."

	POW	POS	DPOS
Introduction	Bitcoin proof mechanism, that is, through the mining to prove. By calculating a hash value that satisfies the rule, you can get the accounting right; send out the data that need to be recorded, after verification of other nodes in the whole network.	An Upgrade Consensus Mechanism of Pow; according to the ratio and time of each node, it can reduce the difficulty of mining and speed up the search for random number.	Like the board of directors vote, the holder of the vote decides a certain number of nodes, agents for their verification and accounting.
advantage	Completely decentralized, free access to the nodes	To a certain extent, it shortens the time for reaching a consensus	Significantly reduce the number of participating verification and accounting nodes, can reach the second level of consensus verification
Disadvantage	At present, bitcoin has sucked bow | most of the computing power in the world, and other block chain applications using the Pow consensus mechanism is very difficult to obtain the Division's computing power to protect their own security; mining caused a lot of waste of resources; the cycle of consensus is longer, which is not suitable for commercial application.	Or need to dig, essentially, there is no solution for commercial application of Painpoint.	The whole consensus mechanism still relies on tokens, and many commercial applications do not need tokens.

Community blockchain (Consortium blockchains)

Refers to the blockchain in which the consensus process is controlled by pre-selected nodes. For example: a community caused by 15 institutions, each organization operates a node, in order to make each block effective, must obtain 10 institutions to confirm. Often referred to as "partial decentralization."

KOK Block Chain Pass

(1) Protect users from developers

Program developers in the public chain do not have the right to interfere with users, so the blockchain can protect users who use the programs they develop.

(2) low access threshold

Anyone with sufficient technical ability can access it, that is, as long as there is a computer that can be

connected to the Internet, the access conditions can be met.

All data is public by default

(3) Although all associated participants hide their true identity, this phenomenon is very common. They generate their own security through their publicity, where each participant can see all account balances and all their trading activities.

4KOK Pass (KOK Block Chain Pass Card) public chain comprehensive application

The public chain of the KOK Block Chain Pass is responsible for data sharing and asset routing between infrastructure and applications. The SDK is responsible for building specific applications.

Application Management:

The application needs to register the meta-information to the main chain before the release. The information includes the name, description, initial witness, and related configuration information required for asset routing. The user can browse and retrieve the decentralized application through the module. Traceability, download and access.

Asset routing:

Assets registered on the main chain can be interoperable (cross-chain) with each application. Although the applications are isolated, the value routing can be achieved through the asset routing function of the main chain.

asset Management:

Any account can register and issue several assets, and the issuer can configure various assets, such as access control lists.

Trustee management:

The trustee is also called a witness. Each holder of the KOK Block Chain Card can be registered as a trustee. The top trustee has the opportunity to become the system's accountant. Forging (or mining, billing, submitting blocks), and obtaining certain token rewards, the trustee can increase the ranking by obtaining the vote of the holder, and each holder can vote for any trustee.

Account Management:

The KOK Block Chain Pass (KOK Block Chain Pass) chain uses an account model. Each private key corresponds to an account. The account stores basic information such as the user's wallet address, public key, nickname, and other configuration or statistical information. The same account model is used in the application chain, so an account on the KOK Pass KOK Pass can directly use the functions of each application.

3.2 KOK Block Chain Card can issue side chains

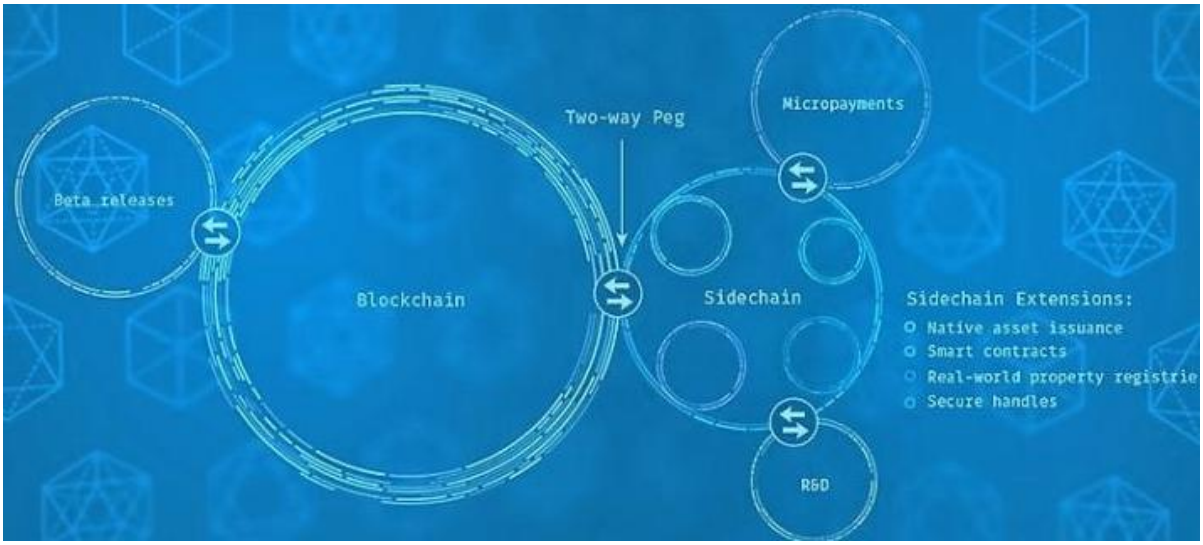
Sidechain(Pegged sidechains), which enable the transfer of bitcoin and other digital assets across multiple blockchains, meaning that users can access new ones with their existing assets The cryptocurrency system. Currently, sidechain technology is primarily developed by Blockstream. The side chain is a special blockchain. It uses a technique called "SPV Wedge" to implement asset transfers with other blockchains, allowing users to use existing cryptocurrency systems with existing assets. People no longer have to worry about Bitcoin's difficulty in adopting innovation and adapting to new demands. Just create a side chain and then connect to Bitcoin's blockchain. By inheriting and multiplexing Bitcoin's powerful blockchain, new ones are avoided. Problems such as the liquidity shortage of money and market volatility. And because the side chain is a separate, isolated system, serious problems in the side chain only affect the side chain itself, which greatly reduces the risk and cost of innovation.

Side chain origin:

Sidechains are not specifically specific to a blockchain, but rather refer to all blockchains that follow the sidechain protocol, which is relative to the bitcoin backbone. The sidechain protocol refers to a protocol that allows Bitcoin to be safely transferred from the Bitcoin backbone to other blockchains and safely returned to the Bitcoin backbone from other blockchains.

Obviously, all existing blockchains, such as Ethereum, can be sidechains as long as they conform to the sidechain protocol. The sidechain protocol is of great significance, which means that Bitcoin can not only be circulated in the Bitcoin blockchain, but also can be circulated in other blockchains, and its application scope and application prospects will be more extensive; creative people will develop A variety of applications interface with the bitcoin backbone with a sidechain protocol, making Bitcoin the stronger the benchmark free currency.

A blockchain is a string of data blocks generated by cryptographic methods. Each block contains information about several network transactions for verifying the validity of its information (anti-counterfeiting) and generating the next block. The user is like a public account book, which records all transaction records, which can be



understood as a distributed database for developers. Blockchain This database is characterized by decentralization,

openness, autonomy, and non-tamperability. Blockchain is closely related to decentralized applications, and is ideal for providing storage functions for decentralized applications.

Side chain protocol:

The purpose of the sidechain protocol is to implement a two-way Peg so that Bitcoin can interchange between the main chain and the side chain (Figure).

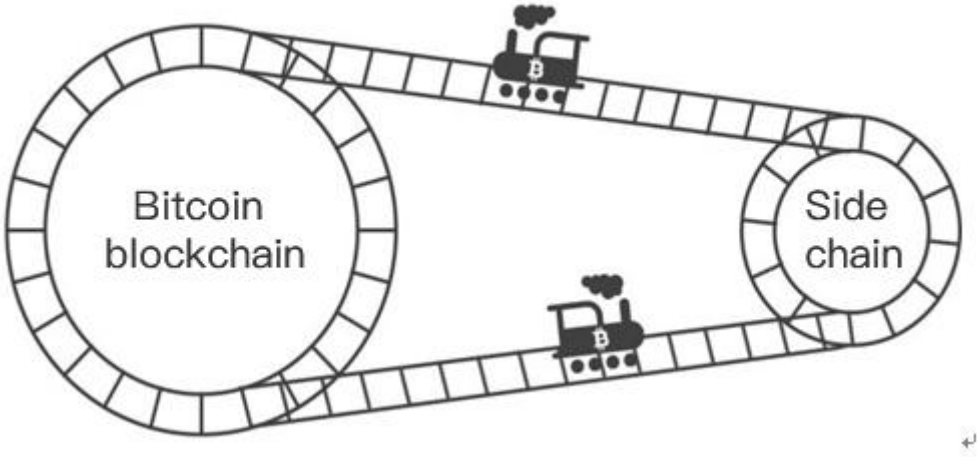


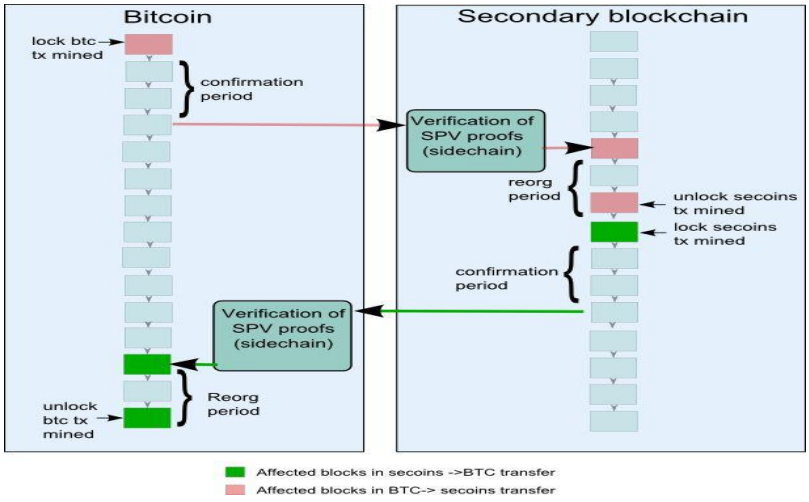
Figure Bitcoin main chain and side chain diagram

Two-way anchoring is divided into the following stages:

Send a locked transaction to lock the bitcoin in the main chain.

Send a locked transaction to lock the bitcoin in the main chain.

Two-way anchoring diagram



- Waiting for a confirmation period

The role of the confirmation period is to wait for the locked transaction to be confirmed by more blocks, to prevent counterfeit lock transactions and denial of service attacks. The typical wait time is 1-2 days.

- Redeem bitcoin on the side chain

At the end of the validation period, the user creates a transaction on the sidechain to spend the output of the locked transaction and provides an SPV workload proof that is output to the address on the sidechain. The transaction is called a redemption transaction, and the SPV workload certification is a proof of the workload of the redemption transaction block.

- Waiting for a competition period

The role of the competition period is to prevent double flowers. During this period (1) the redemption transaction will not be packaged into the block. (2) The new bitcoin transferred to the side chain cannot be used. (3) If there is a work permit with a larger workload, that is, the redemption transaction includes The more difficult SPV proof of the Bitcoin main chain, the last redemption transaction will be replaced。

The role of the side chain:

Sidechains allow blockchains to achieve better performance and privacy protection. They can also scale to support a variety of assets, such as stocks, bonds, real-world or virtual world currencies, as well as smart contracts, security processing, and real-world property registration. The side chains can also have other side chains for micropayments. They can be used for experiments with pre-release versions of future sidechains, or for experiments with Bitcoin test versions.

3.3 Technical Status: Complete Script vs Side Chain

One of the highlights of Bitcoin's design is its scripting engine. Based on this scripting engine, not only can the ordinary transfer function be realized, but also smart contract applications such as multi-party signature, mortgage guarantee, and gaming. However, for the sake of security and implementation difficulty, Bitcoin's scripting system is designed to be relatively simplistic and imposes many restrictions. For example, it does not support loops, script length is limited, and only supports several standard transaction types.

The biggest feature of Ethereum is that it greatly expands the function of this scripting engine. It adds new instructions such as reading blockchain, billing, and jumps, and also removes stack memory, function call depth, and script length limits. Ethereum claims that their scripting language has reached Turing's completeness, and with such scripts, developers can implement almost any mathematically expressable function.

Since Ethereum, extended scripts have become a popular way to implement decentralized development platforms, but this approach has a big disadvantage: the application code itself and the data generated by the application are in the same blockchain. Caused a rapid expansion of the blockchain. Ethereum tried to delay this expansion by optimizing and compressing the block and the transaction itself, and it was just a way to cure the problem. In addition, the script-based applications share the same book, and parameters such as block generation time cannot be customized, which undoubtedly limits the personalization of the application.

The sidechain mechanism is scalable through another dimension, each running on a different distributed node network with separate audiences, investors, and development teams. This natural sharding solution not only solves the problem of blockchain expansion, but also has a personalized set of books for each application. The consensus mechanism, block parameters, and transaction types can all be customized. We believe that sidechains are a lower cost, more flexible, and easier to use solution than full trading scripts.

3.4 relational database vs non-relational database

At present, most blockchain systems choose to use a simpler non-relational database to store data, such as berkeley db, leveldb, etc. These databases generally provide some simple data structures, such as btree, hashtable, queue, etc. SQL is not supported for data manipulation. Although these databases are sufficient for general electronic money systems, they are not enough for application platforms, especially for financial, banking, e-commerce, and other mainstream storage. The system uses a relational database because relational data has several advantages:

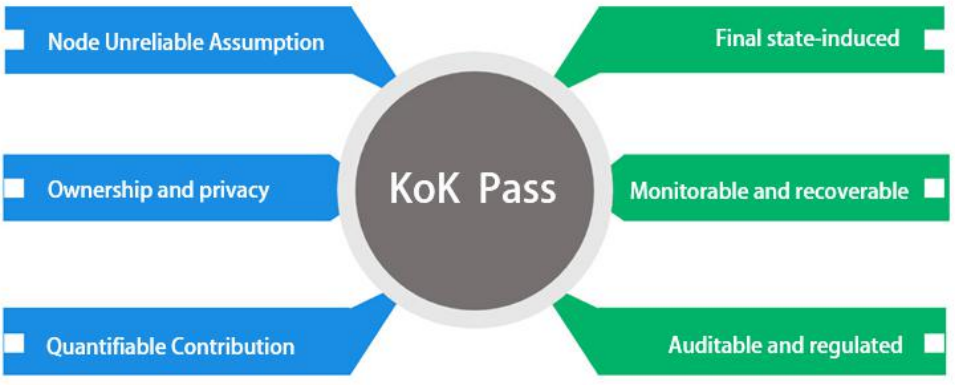
- transaction processing
- Data update overhead is very small
- can perform complex queries such as join

The sqlite we chose is a lightweight, lightweight embedded relational database with up to 2T capacity.

3.5 KOK Pass Chain Card Technical Design Principle

Node unreliable assumptions:

Based on a loose network organization, single points of failure and nodes are allowed to be unavailable for a certain period of time. But the whole network still needs to have strong robustness.



Ownership and privacy:

The data owner has ownership and full access to the data, and the data is encrypted and private. Other roles can access and use data after authorization by the owner.

Quantitative contribution:

The contribution of all parties involved in the agreement should have corresponding quantitative criteria and contributions that can be observed. For example, POS and POW are used as quantitative proofs of storage space and storage time.

Final state consistency:

Allow data objects to be in different states on different nodes, but their final state can quickly converge to achieve network-wide consistency.

Monitorable and recoverable:

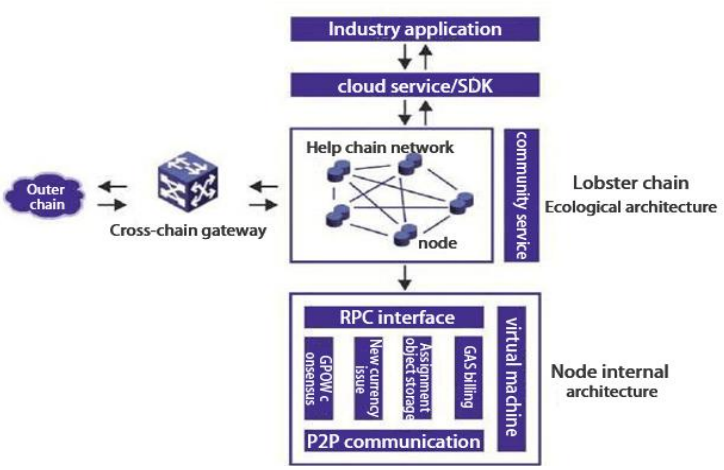
It can detect the availability of the entire network, the state of the entire network of data objects, and repair it to a certain extent according to the corresponding strategy.

Auditable and regulated:

A certain degree of supervision and auditing can be performed in certain specific areas or scenarios, provided that the data owner is aware of and willing to be in such a regulatory framework.

Store data under the shelf.

3.6 KOK Block Chain Card Technical Architecture



The "KOK Pass" provides a complete distributed ledger system, including a complete smart contract system and security system. At the same time, the “KOK Pass” abstracts the underlying complex technical system and heterogeneous systems, supports distributed entity management and multidimensional authentication protocols that are compatible with various major protocols and cryptographic standards, and supports heterogeneous blocks. Cross-chain, cross-system interaction mapping between chains and traditional information systems. The “KOK Pass” also provides technical systems such as secure data storage, heterogeneous smart contracts, hardware key management, and encrypted data analysis. The entire network as an application platform can support the construction of various application services, especially decentralized applications. On this basis, “KOK Pass” provides a series of application frameworks, including distributed data exchange protocols, distributed process

management protocols, etc., and further supports the implementation of various upper-layer applications through common APIs, SDKs and various application functional components.

"KOK Pass" underlying SDK

The KOK Passchain is responsible for data transfer between infrastructure and applications, as well as asset routing, and the SDK is used to build specific applications.

ORM supports object-relational mapping to organize business data, supports index configuration, and performs complex queries through JSON syntax.

JavaScript uses JavaScript as a native language, and developers can use a large number of third-party components to freely combine.

The Two-way peg cross-chain protocol supports bidirectional anchoring of cross-chain protocols.

Immutable ledger built-in ledger creation function, developers and users only need to call the contract, all call operations and status will be automatically written to not falsify the ledger.

Lower level interfaces Compared to Ethereum's Solidity language, KOK Pass allows developers to use more underlying interfaces to maximize control of the system, such as handlers and filters for lifecycle events.

Customize fee definitions developers can set different fees for each transaction or contract, and even set different asset tokens as a handling fee, not limited to KOK Pass KOK.

Transaction privacy optional transaction privacy feature.

SmartDB caching is automatically synchronized with persistent storage to dramatically improve write performance.

Chapter IV Cryptography of KOK Pass

4.1 KOK Pass relies on the cryptography of KOK

4.1.1 Asymmetric encryption

An asymmetric encryption algorithm requires two keys: a public key (publickey) and a private key (privKOKekey). The public key and the private key are a pair. If the data is encrypted with the public key, only the corresponding private key can be used for decryption; if the data is encrypted with the private key, only the corresponding public key can be used. Decrypt. Because encryption and decryption use two different keys, this algorithm is called an asymmetric encryption algorithm.

Working principle / asymmetric encryption

1. A wants to send information to B, both A and B generate a pair of public and private keys for encryption and decryption.

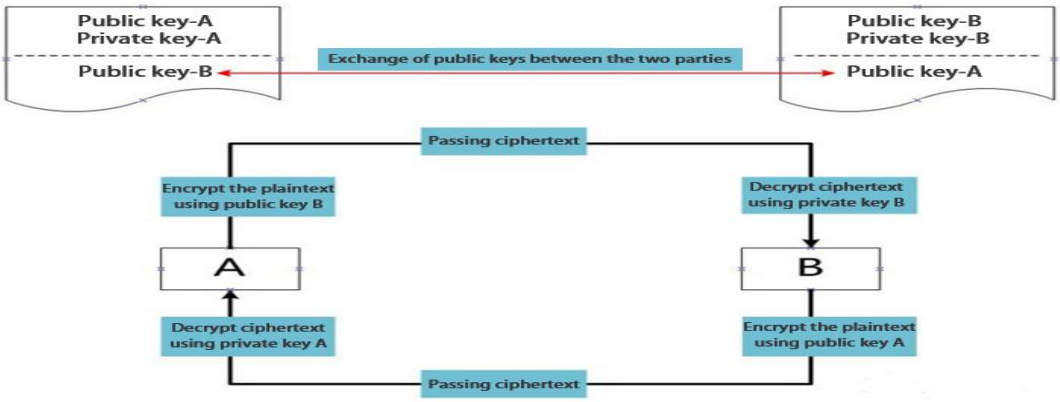
2. A's private key is kept secret, A's public key tells B; B's private key is kept secret, and B's public key tells A.

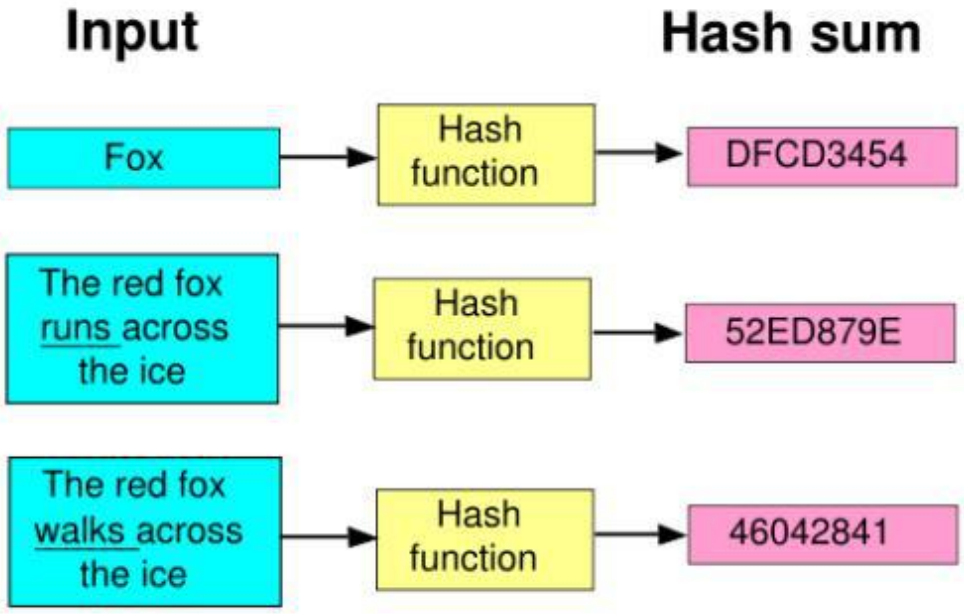
3. When A wants to send information to B, A encrypts the information with B's public key because A knows B's public key.

4. A sends this message to B (the message has been encrypted with B's public key).

5. After receiving this message, B decrypts the message of A with his private key. Anyone else who receives this message cannot decrypt it because only B has the private key of B.

4.1.2 Hash Algorithm





4.1.2.1 Hash Algorithm Definition

Hash Algorithm, also known as hash algorithm, hash algorithm, is a way to create small digital "fingerprints" from arbitrary files. Like a fingerprint, a hashing algorithm is a sign that guarantees the uniqueness of a file with shorter information. This flag is related to every byte of the file, and it is difficult to find the inverse law. Therefore, when the original file changes, its flag value will also change, thus telling the file user that the current file is not the file you need.

4.1.2.2 Application of Hash Algorithm

SHA256

SHA256 is a member of the SHA (Secure Hash Algorithm) family. SHA-256's calculation process is divided into two phases: message preprocessing and main loop. In the preprocessing stage of the message, the filling and expansion padding of the message is mainly completed, all the input original messages are converted into n 512-bit

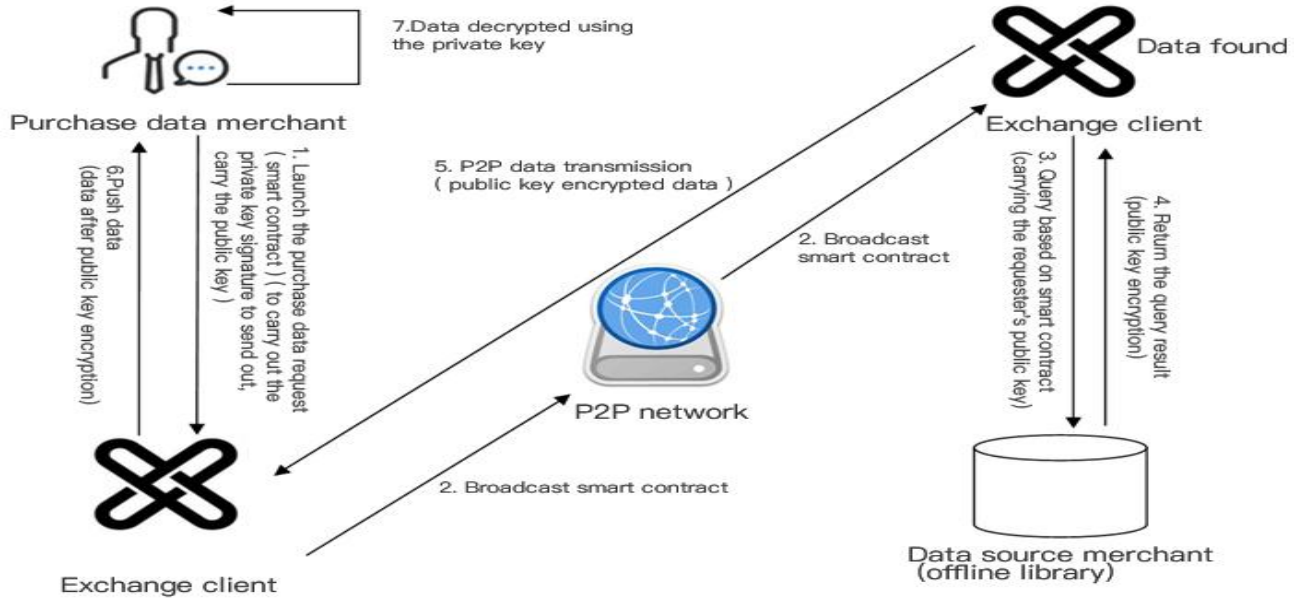
message blocks, and then each message block is processed by the SHA256 compression function.

Merkle Hash Tree

A Merkle hash tree is a type of hash-based binary tree or multi-fork tree. The value on the leaf node is usually the hash value of the data block, not the value on the leaf node. It is the child node of the node. The hash value of the combined result. Merkle trees are generally used for integrity verification processing. In the application scenario that handles integrity verification, the Merkle tree greatly reduces the amount of data transferred and the complexity of the calculation.

4.2 Application of Cryptography in KOK Pass

Take the data transfer of a data buyer node and a data source node as an example to explain this problem:

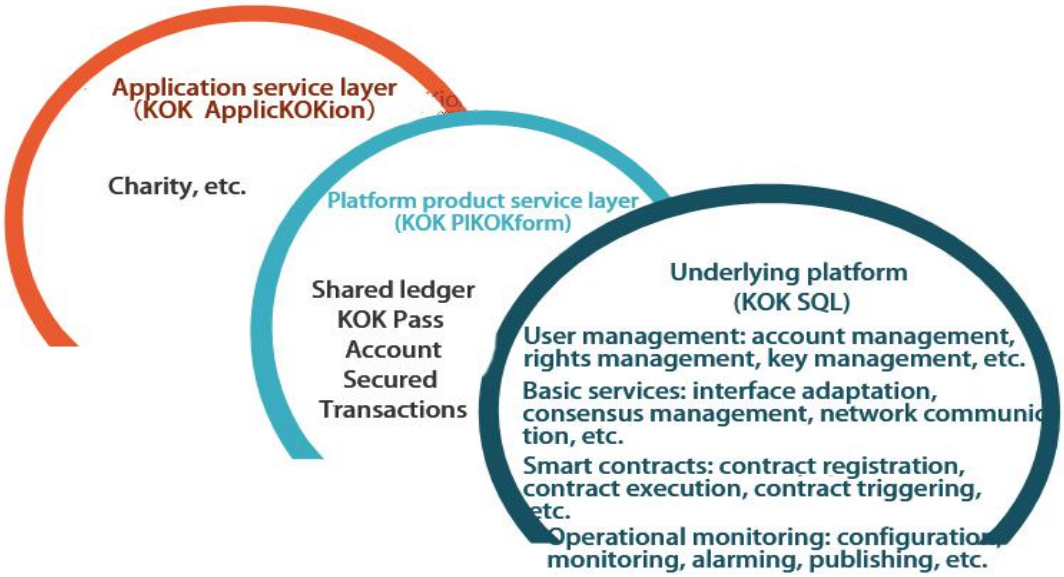


Merchant A who purchases the data, private key signature of the smart contract (the private key is generated by the merchant on his own client in his own way, and it cannot be obtained by the person), and carries his own public key when transmitting, and broadcasts through the exchange client. To the whole network node, the data source merchant node in the above figure receives the broadcast, and invokes the data interface of the data source to query. If the data source queries the data, the source data is encrypted by using the public key of the merchant A, and then transmitted to the merchant A point-to-point. The client node, the client node of the merchant A pushes the data to the receiving data interface of the merchant, and the merchant A uses the private key to decrypt the source data. The whole process uses asymmetric encryption. The encrypted data uses the public key of the merchant A, and only the private key of the merchant A can be decrypted. Even if the data packet is intercepted by others, the data cannot be unlocked (even if the KOK pass is intercepted because No private key can not be solved), completely guarantee the transmission security of the data transaction process.

Chapter V Technical Structure

5.1KOK Pass Overall Architecture

Under the guidance of the public chain design principle, the overall structure of the KOK Pass is divided into three levels: the bottom layer of the KOK Pass is the KOK SQl platform independently developed by the KOK Pass, and the KOK SQL provides the blockchain foundation for the upper application scenarios through the interface of SQL and API. The function of the service. The core is to create an efficient charity block



In the middle, the platform product service layer is KOK PIKOKform, which builds high-availability and scalable blockchain application base platform products on the underlying (KOK SQL), including shared accounts, KOK passport accounts, secured transactions, digital assets, etc. In one direction, integrating basic product functions in related fields to help philanthropy quickly build upper-level blockchain application scenarios. The application service layer (KOK ApplicKOKion) provides the trusted, secure and fast blockchain application to the final believers. In the future, KOK Pass will work together with industry partners to explore the development direction of the industry blockchain and jointly promote the application of blockchain application scenarios.

5.1.1KOK SQL underlying platform

User management: responsible for the identity information management of all chain participants, including maintaining public and private key generation, key storage management, and maintaining the user's true identity and KOK passport address correspondence, and supervising and auditing certain real identities under authorization. Trading situation. For the application of financial transactions such as digital assets, it also provides rules for risk control to ensure system transaction security.

Basic Services: The basic services are deployed on all KOK Pass nodes to verify the validity of the business request and to record the valid request and record it on the storage. For a new service request, the basic service first parses the interface, authenticates the process, and then registers and encrypts the transaction or contract through the consensus algorithm, and then stores it completely and consistently on the shared ledger. The consensus mechanism is adaptive, and has high concurrency in the normal case of network and nodes, and is highly fault-tolerant in the case of network anomalies or node spoofing.

Smart Contract: Responsible for the registration and issuance of contracts and the triggering and execution of contracts. The user defines the contract logic through a programming language. After posting to the KOK Pass, the logic of the contract terms is triggered by the user's signature or other events to complete the logic of the contract for settlement of the transaction.

Operational monitoring: Responsible for deployment, configuration modification, contract setting, and output of real-time status visualization during product release, such as alarms, transaction volume, network conditions, and node health status.

5.1.2 Platform Product Service Layer KOK PlKOKform

The platform product service layer abstracts various typical KOK passport applications, providing basic capabilities and implementation frameworks for typical applications. Based on these basic capabilities, users can superimpose the unique features of their own business and easily implement the KOK Pass for business logic. Help users quickly relocate existing services to KOK Passes to meet new scenarios, or build new business scenarios, and use KOK Passports to solve problems that were difficult to solve before.

Digital assets: Based on the analysis of digital assets such as virtual currency and commercial paper, we find that asset chaining is a key link. To this end, the concept of “asset gateway” is introduced to assist users in the transformation of assets under the chain to assets on the chain. Once the assets are on the chain, operations such as transfer, splitting, and withdrawal will be strictly controlled through the account public and private key system, and all operations will have signature verification. Both sides will leave traces and cannot be erased. For example, commercial notes and other assets with valid periods will also provide automatic liquidation at maturity, including asset issuance, asset transfer, asset withdrawal, asset liquidation, and asset inquiries.

Forensic Services: For application scenarios such as intellectual property rights, policy preservation (certificate of equity), personal and corporate qualification certificates, KOK Passes fully exploit the indelible and publicized capabilities, allowing organizations and individuals to use a simple interface or APP client. Publish copyright information, insurance information, qualification certificates, etc. to the KOK Pass, and let all the accounting nodes testify for themselves. In addition, based on the self-built platform, the user's rights protection will be more convenient, and the evidence confirmation is more authoritative. Such as ownership registration, ownership cancellation, infringement evidence entry, etc.

Shared ledger: The reconciliation between financial institutions is basically carried out on a daily basis. The

reconciliation method is basically a mutual reciprocal statement, which compares the transaction flow between the two parties. This brings a certain delay to the final transaction confirmation and fund transfer. Some business scenarios that require real-time payment must even be carried out by the business operator. The natural shared account book of KOK Pass allows the reconciliation to be sent in the next day, but can be carried out at any time. Both parties can complete the reconciliation of funds by simply dialing the reconciliation logic to the KOK Pass. Basically, real-time transaction confirmation and fund transfer can be realized, and neither party can be denied. Especially for the long-term capital chain, the business involving more links has a competitive advantage. At the same time, the regulator can also participate in the shared ledger record.

Sharing the economy: A key factor in the long-term sharing of the economy is the establishment of trust between the supply and demand sides to ensure the smooth implementation of the sharing behavior, and the KOK Pass provides a way to achieve the technical level. The endorsement of technical guarantee capability enables multiple participants who are difficult to achieve mutual trust to establish credibility, no need for intermediate institutions or service platforms to build a strong internal audit process, rigorous and complicated accounting backup system, and coordination with regulatory agencies. With the extra facilities, you can achieve the same effect. This saves a lot of cost and makes sharing more efficient and feasible.

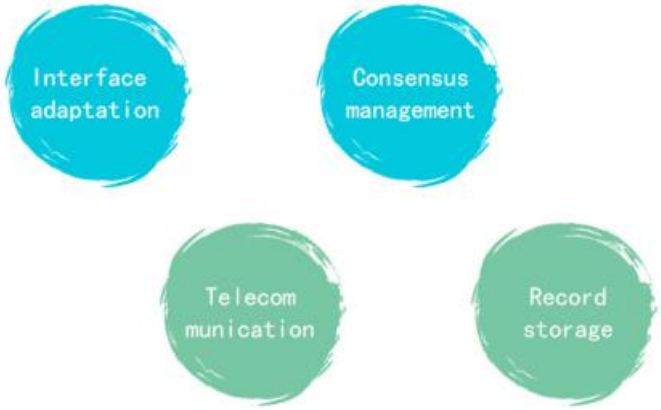
5.1.3 Application Service Layer KOK ApplicKOKion

The application service layer (KOK ApplicKOKion) provides application services based on the KOK Pass scheme to end users. In the KOK Pass Solution, the application service layer will try its best to provide users with various KOK Passport scenarios. In the future, we will provide users with reliable, secure and convenient blockchains in the fields of digital bills, network mutual assistance, institutional clearing, and public welfare. service. KOK Pass will also be based on the principle of open sharing. In the future, we will work together with various industry partners to explore more application scenarios of sidechains, and open up the capabilities of KOK Pass and KOK PlKOKform to jointly develop new applications. Service, together with the maintenance of the KOK Pass Ecology.

5.2KOK SQL underlying platform

5.2.1 Basic services

The basic service module consists of four parts: interface adaptation, consensus management, network communication and record storage.



Basic services

5.2.1.1 Interface Adaptation

For convenient and low-cost access to KOK passes, KOK SQL provides SQL and API interfaces to the application layer. The API interface supports both synchronous and asynchronous modes. After the interface adaptation layer parses the service request, after the authentication and signature verification, the service request is recorded to the account book through the consensus algorithm. As an client of the consensus management module, the interface adaptation module also participates in consensus management. The interface adaptation module is mainly responsible for the summary and consistency judgment of the results returned by each consensus node. In addition, when the "improved bft-raft" consensus algorithm with independent intellectual property rights is used, the interface adaptation module also receives the election switching request from the service side, and the interface adaptation module summarizes the election switching request. When the switching condition is met, the consensus management module is notified to re-elect.

5.2.1.2 Consensus Management

The consensus mechanism is the core technical point in the KOK Pass. A process in which a multi-party node agrees on data, behavior, or process through interaction between nodes under a preset rule is called consensus. The consensus mechanism refers to the algorithms, protocols, and rules that define the consensus process.

The consensus mechanism is divided into two categories according to the consensus process. The first category is the consensus with consistent probability and the final confirmation in engineering; the second category is the consensus after absolute agreement, and the consensus is confirmed. The KOK Pass provides a second type of consensus mechanism that supports both adaptive and user-specified configurations. The adaptive mode is an "improved raft" algorithm with automatic consensus, high efficiency, fraud prevention, and independent intellectual property rights when the network is in good condition and has no fraudulent nodes. When the fraud node or the faulty node exceeds the threshold, it automatically switches. To a more rigorous "improved bft-raft" algorithm with independent intellectual property rights. User-specified configuration mode means that the user directly configures a fixed consensus mechanism for consensus management.

5.2.1.3 Network communication

The network communication module is responsible for message data transmission between nodes and on the service side. The KOK Pass uses a dynamic, self-organizing network that can be multiplexed and connected for sharing. It can be compatible with existing security facilities such as firewalls and proxy servers, providing peer-to-peer networking and secure and reliable data transmission.

5.2.1.4 Record Storage

KOK Pass record storage can support the storage of a variety of media, storage media can be a database, file system, or cloud storage media, such as cloud DB, cloud KV and so on. Record storage uses a blockchain structure, any tampering with historical data can be found by self-checking, and alarms and automatic corrections.

Block body	Block body	Block body
All transaction information in the secondary block	All transaction information in the secondary block	All transaction information in the secondary block
Block height: 390608	Block height: 390609	Block height: 390610
Head hash: 00000000005ele25	Head hash: 00000000003f2f1d	Head hash: 00000000002c8ae5
Head hash: 000000000079f...e4d	Head hash: 0000000000sfel...e25	Head hash: 00000000003f2...f1d
Merkle root 2el1abce579.e12a	Merkle root c59e2d8242.ef1c	Merkle root c8572f19112.456d
Difficult: 93448670796.32380676	Difficult: 93448670796.32380676	Difficult: 93448670796.32380676
Ncnce: 2181060612	Ncnce: 4005489007	Ncnce: 1779633802

Blockchain data section

5.2.1.5 Database

According to the data structure organization form of the database, it is generally divided into Key-Value type and relation type. Among them, Key-Value database has a simple data structure organization structure, high read and write performance, can support massive concurrent read and write requests, and has strong scalability, simple operation interface, and supports some basic read, write, modify, and delete. Other features, but do not support complex SQL features and transactionality. The relational database uses a relational model to organize data, supports various SQL functions, is highly functional, supports transactionality, has general read and write performance, and is weak in scalability.

According to the deployment form of the database, it is generally divided into two types: single type and distributed type. Among them, the stand-alone database guarantees strong consistency and good usability. Distributed databases follow a distributed architecture in physical deployment, providing high concurrent read and write performance and fault tolerance, strong availability and partition fault tolerance, but the data consistency of the distributed architecture is weak due to the need for data synchronization. Only the final consistency can be guaranteed.

The sqlite selected by KOK Pass is a lightweight and lightweight embedded relational database with a maximum capacity of 2T. The data files can be shared freely between different endian machines, especially for SQL. It will be developed for dapp. Provide great convenience.

KOK SQL

5.2.2 User Management

User management mainly solves the mapping relationship between user identity and KOK passport address, the confidentiality of user privacy, and the traceability of regulatory audit. From the business scenario, some scenarios require anonymity, transactional irrelevance, such as digital currency, etc. Some scenarios do not require anonymity and irrelevance, such as source tracking, charity and so on. To balance these two scenarios, key management requires strong adaptability and compatibility. The KOK Pass provides a variety of configurations that users have the flexibility to choose.

From the perspective of user access, one is that the original system is modified to access the KOK pass, and there is a key management system with a high security level, such as institutional clearing, bank factoring, etc., and the other is a new application scenario. There is no perfect key management system for entering the KOK Pass or the original system. In order to inherit the key security management system with high security level and retain the usage habits of the original users, KOK Pass provides three types of traditional key system integration, full hosting and partial hosting.

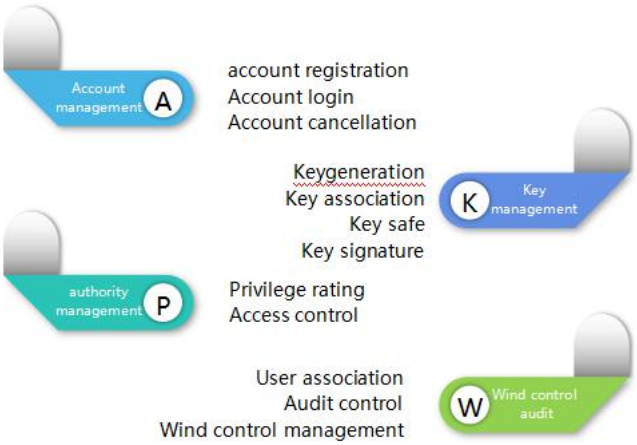
Traditional key system integration: It is suitable for users with high security level of the original private key system, such as: financial institutions, original U shields of the bank, electronic signatures, etc. For such users, KOK passes only need to be used by the original users. The private key system is associated with the KOK Passport address.

Partially managed: Some subjects that access the KOK Pass service have a higher security level key system or multiple KOK Pass technology interworking scenarios. In some cases of hosting, the KOK Pass guarantees the multi-party KOK Pass address association and consistency of participation.

Fully hosted: A scenario suitable for new access and a scene with a high degree of customary Internet usage. The original system of username and password is associated with the secure key generation and management system to isolate the user information from the KOK passport address and protect the privacy of the user.

For the fully managed mode, the user management system of KOK Pass consists of account management, key

management, authority management and risk control audit.



User Management

5.2.2.1 Account Management

Account management is responsible for user account management, including account registration, login, logout, and account and key irrelevance processing. When the account is registered, the identity information such as the user name and password that the original user is accustomed to is mapped to the KOK passport address. After the account is logged in, the KOK Pass related business request can be sent. For scenarios with high transaction confidentiality, the user can select the KOK passport address irrelevance processing, so that different transactions of the same user are not related in the block record storage, which improves user security and transaction confidentiality.

5.2.2.2 Key Management

In the fully managed mode, the key management system is responsible for the association of the user key with the account, key security management, and loss recovery. The user key is generated on the client, and the user can choose to save the key in the key safe or delegate to the associated account so that the key is lost and retrieved. In order to ensure the reliability of the association relationship between the user account and the key, the key management system uses the multi-node chain storage for the signature of the association relationship.

5.2.2.3 Rights Management

The rights management module is responsible for the control and management of user accounts, key systems, node joins and exits, and data access. Including audit permissions, account delegation permissions, node consensus permissions, and user data access permissions. Auditing authority is the function of providing auditing to the regulatory authorities, access rights and data scope.

With strict control, users who are unrelated to transactions on the shared ledger can do user associations. The account delegation authority is used to control the access control of the user account delegation relationship. Consensus authority for consensus authority management for participating or newly joining nodes. Access rights are used to manage client-side data query permissions on KOK Pass.

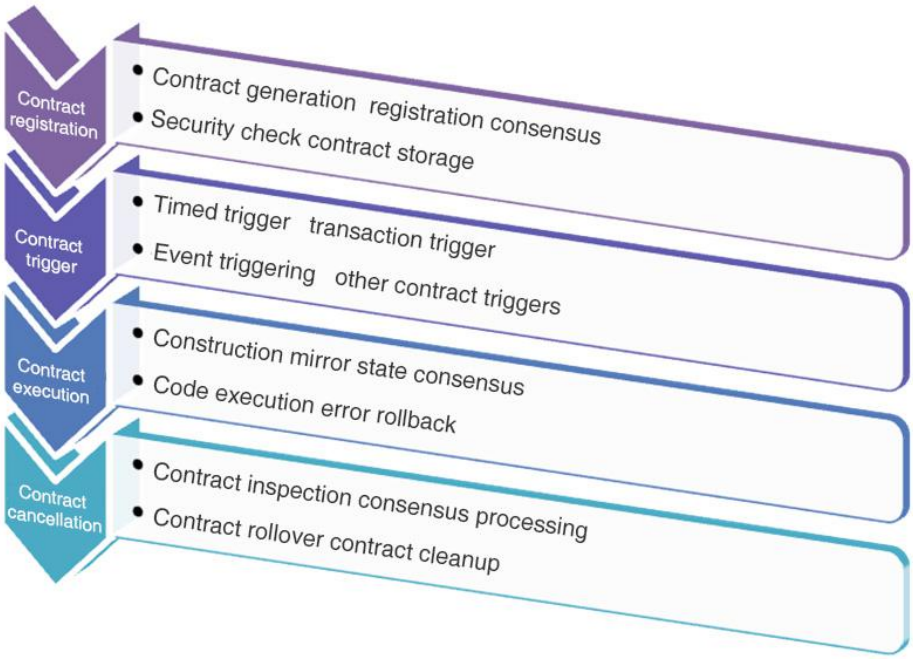
5.2.2.4 Wind Control Audit

The wind control module is responsible for risk control of the trading behavior of digital assets in the KOK Pass. The KOK Pass Chain provides a risk control expert model system. By analyzing and capturing the deep relationship between massive data, the risk control rules are adaptively adjusted, and risks are discovered in time. Manage risk control and control risks to prevent problems before they happen. The audit module provides auditing capabilities to the auditing organization and ensures that auditing capabilities can only be used by the auditing organization through strict authority controls.

5.2.3 Smart Contract

The blockchain contract section includes both standard contracts and business-customized contracts. Standard contracts include asset consistency check, automatic transaction matching, multi-party confirmed transfer, automatic clearing of accounts, etc. The relatively simple contract is a KOK Pass built-in contract that can be directly linked to the KOK Pass. User-customized smart contracts include the ability to modify configurations and add other business logic through contract templates, as well as support for more complex user-programmed contracts that run in a stand-alone environment.

Smart contracts include the registration, triggering, execution, and cancellation of



Smart contract

Contract registration

Contract registration is the process of storing the consensus to the KOK Pass after the user has prepared a contract security check.

- **contract trigger**

Contract triggering is the process of triggering contract execution through external conditions after contract registration, supporting timing triggers, event triggers, trade triggers, and other contract triggers. Timing triggering refers to the process of automatically triggering a contract call after the node triggers the time consensus after the preset time in the contract is met. Events, transactions, and other contract calls are triggered by a new request consensus process.

- **Contract execution**

Contract execution is the complete process of running contract code in a separate environment, including a contract construction environment, code execution, consensus on state changes in the execution code, and consensus exception handling.

- **Contract cancellation**

Contract cancellation is the process of dumping, cleaning, and cleaning up contracts that have been executed, expired, or changed in business requirements. The process of cleaning up and cleaning up requires multiple nodes to complete.

5.2.4 Operational Monitoring

In order to quickly access and access the system, the system can quickly and accurately identify the running status of the system and meet other operation and maintenance requirements during operation, such as storage

account expansion and program upgrade. KOK Pass provides a complete, fast and visualized operational monitoring system. Operational monitoring mainly includes configuration, monitoring, alarming, publishing and business analysis functions.

5.2.4.1 Configuration

Responsible for processing the relevant configuration of the network node, such as the selection of the consensus algorithm, the adaptive threshold, the storage method of the storage book, the network routing mode, etc., the configuration itself can be issued as a transaction in the KOK passport, and agreed by the consensus algorithm. Then take effect.

5.2.4.2 Monitoring

Responsible for collecting state data running in the system and visualizing it. The status data in the system includes the system's access volume, time-consuming, node health status, and comparison of the underlying machine resources (CPU, memory, hard disk) usage status, etc. Through visual monitoring, the status of the entire KOK passport system can be known in real time.

5.2.4.3 Alarm

The serious situation in the system, such as fraudulent nodes, account tampering, machine failure, etc., is notified to relevant personnel through SMS, telephone, WeChat, email, etc., so as to be processed in time.

5.2.4.4 release

Operations in scenarios such as system initial deployment, running program upgrades, and node extensions during runtime can be supported through the release module. The publishing module guarantees the consistency of executable programs of important modules such as interfaces and consensus algorithms.

5.2.4.5 Business Analysis

Business analysis includes data consistency detection between nodes and multi-dimensional statistics and analysis of transaction data, which can provide specific authorized users with charts for business statistics analysis and business development trends.

5.2.4.6 Cloud Adaptation

The cloud adapter provides the interface adaptation of the current mainstream cloud operators, which makes the KOK passport more convenient to be deployed on the cloud for maintenance and expansion.

5.3 KOK Pass Distributed Book Technology

A distributed ledger is a database that is shared, replicated, and synchronized between network members. A distributed ledger records transactions between network participants, such as the exchange of assets or data. Participants in the network constrain and negotiate updates to records in the book based on consensus principles. There is no involvement of intermediate third party arbitration institutions (such as financial institutions or clearing houses). Each record in the distributed ledger has a timestamp and a unique cryptographic signature, which makes the ledger an auditable history of all transactions in the network. One implementation of distributed ledger technology is the open source Hyperledger Fabric blockchain.

In the KOK Pass, the use of distributed ledger technology will be further expanded in the following areas:

1 Real name registration and identification:

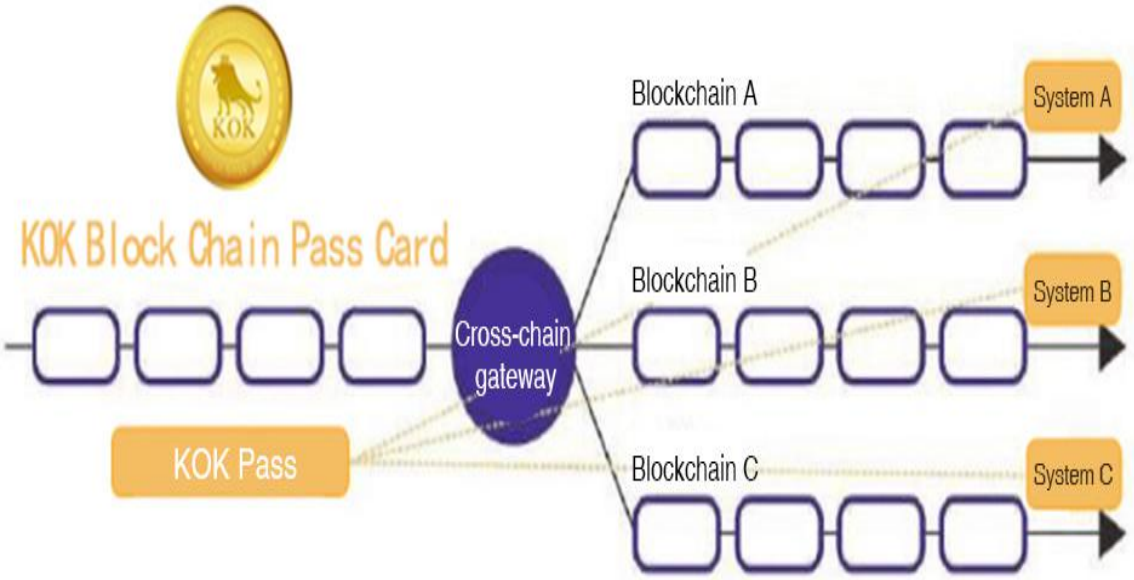
Entity identity registration and identification is an important basic module of the “KOK Pass”. The “KOK Pass” has designed a multi-faceted, multi-level registration, certification and authorization system for participants and related resources. The entity identity and authorization module is designed to provide a multi-level identity authentication and authorization system. By flexible configuration and integration of its own authorization service or third-party authentication mechanism (such as CA authentication), it is also possible to conduct community-based implementation of various types of account ontology. Endorsement of certification, and integration of different audit mechanisms according to business scenarios, systemized identity authentication and authorization for blockchain participating nodes and participants.

2 Data directory:

Using distributed ledger technology, catalogues can be registered for the provided data categories, and the unique identification of the data (ONT DKOKa ID) and the data resource acquisition address (DKOKa URI) can be matched to match the required data to the required data. The comparison of ONT DKOKa ID data deposits determines the validity of the data.

3 Data exchange:

Using distributed ledger technology, it can realize the data exchange framework based on entities (people, things, equipment, content...), revitalize personal data assets, enable data to be used in circulation, and support data discovery and authorization with standardized protocol design. And transactions, to help users to fine-grain the data, to meet the user's own privacy needs while seeking the benefits of data reuse.



4 Process synergy:

Process collaboration (distributed transactions) using distributed ledger technology, entity cross-chain and cross-system privacy, and specific cross-chain protocols. That is, multiple steps of the process/transaction are distributed on different blockchains or systems to ensure the identity privacy of different entities in different systems and blockchains, and to ensure the consistency of the entire transaction.

5 Behavioral Deposit and Smart Contract:

Through the use of distributed ledgers, more than just providing data deposits, and through the support of smart contracts, different businesses can conduct more business flows to support the deposit. That is, each time data request, data matching, data process expansion and innovation, in the business process coordination, control and exchange, etc., the establishment of the transfer and the use of data are recorded in the ledger, forming a data-specific technology. Trust mechanism. The record of the process ensures that the data is safe, reliable and not leaked.

5.4 KOK Pass Code Data Exchange System

The KOK Pass provides a range of underlying features and protocol support for distributed data exchange.

1 Distributed Data Exchange Protocol:

The “KOK Pass” will be compatible with supporting multiple different types of global data exchange protocols to support different business scenario requirements, while combining data exchange protocols with distributed ledgers to form distributed data exchanges.

Change the process and provide support for a range of data and privacy-protected cryptographic components.

2 Data authorization mechanism:

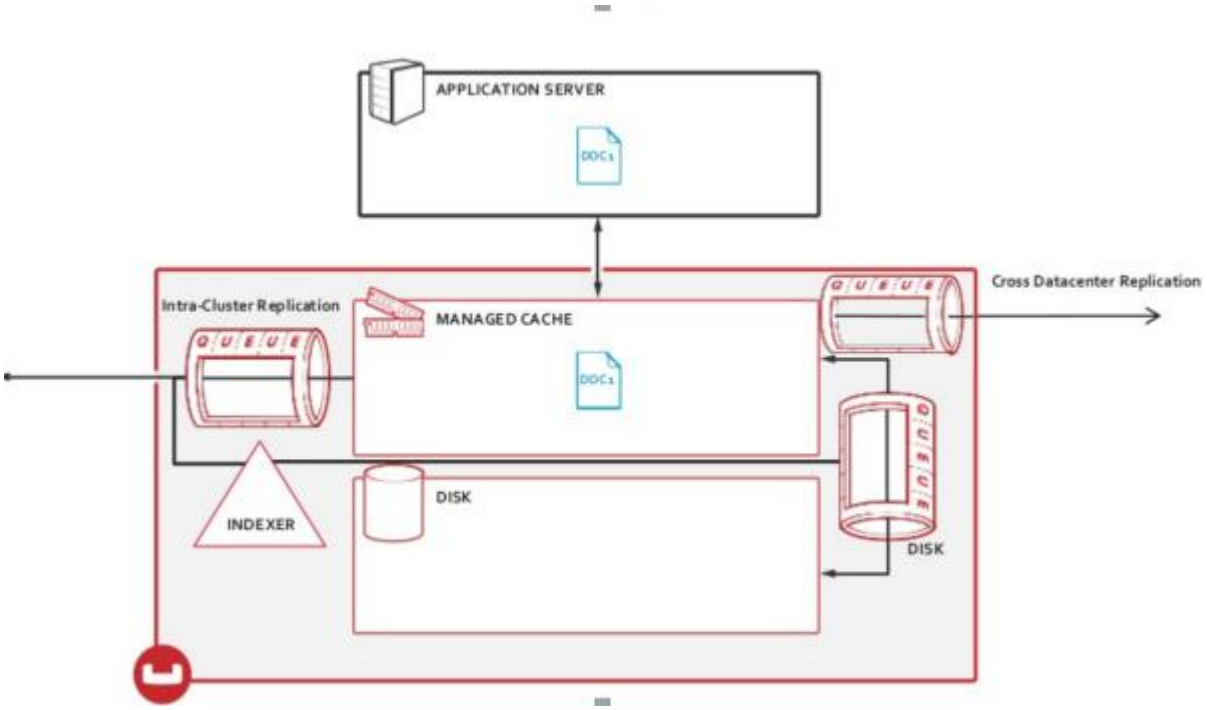
In the data exchange system, data privacy protection and data leakage prevention are always the focus. In the trust ecology established by the “KOK Pass” network, an authorization mechanism is designed, that is, any

transaction involving data related to the data subject, and the data stakeholders (single or multiparty) need to be notified to conduct the authorized transaction.

3 Copyright protection of data:

In response to the digital nature of data, the “KOK Pass” provides data deposit and lifecycle management functions, and designs a lifecycle traceability mechanism for related data. First, the digital identity is established for each data to track the whole process of registration, request, authorization, transaction, etc. Secondly, the copyright protection of data and the transaction of data are recorded in the distributed ledger.

4 Distributed storage of data: Provide a distributed data storage layer that supports data exchange and support various data applications.

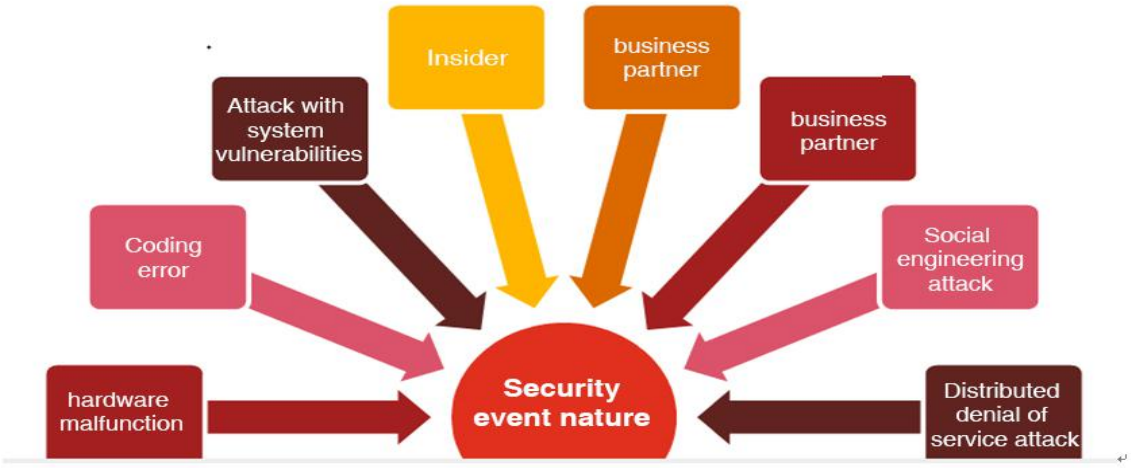


5 cryptography technology and data protection component Ontology Crypto Package (OCP):

In multi-dimensional entity authentication, distributed data exchange, distributed process protocols, etc., the "KOK Pass" network provides a series of cryptographic and data security component support, including data encryption transmission, key sharing protocol, multi-party key Management, ring signature component, blind signature component, threshold sharing mechanism. In the identity and data verification process, zero-knowledge proof and homomorphic encryption scheme are provided. In the data collaborative application process, two-party computing is provided, and the multi-party technical solution is further explored in the future. In addition, the “KOK Pass” provides specific security components for specific scenarios and supports upper-level application implementers to build applicable security application protocols based on security components.

Chapter VI KOK Pass Technical Architecture Security and Network Security Protection

6.1Thesecurityadvantagesoftheblockchain itself

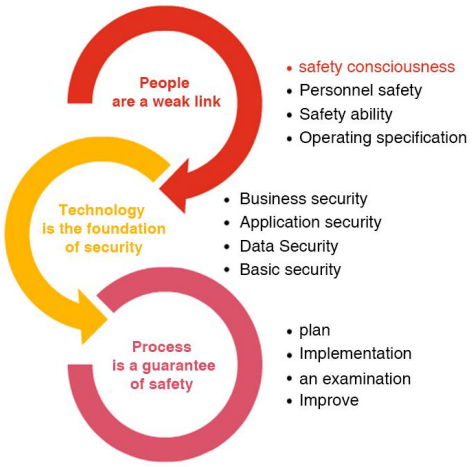


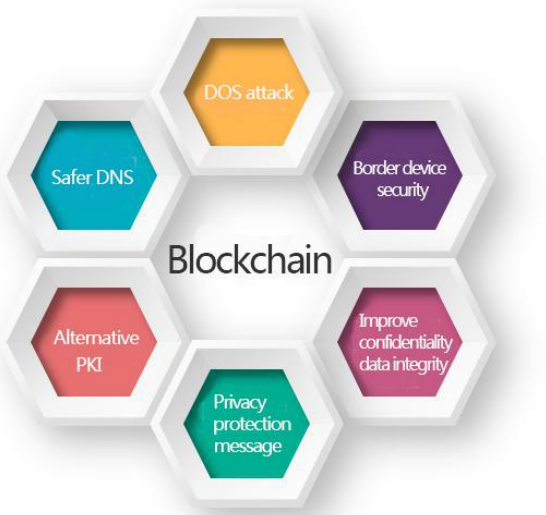
6.1.1 Blockchain security advantages

Today, hackers can disrupt the entire network, tamper with data, or induce careless users to fall into a security trap. They steal identity information and cause other security threats through attacks on centralized databases and single points of failure. However, the pattern of data storage and sharing of data in blockchain technology is quite different from current information security. Both Bitcoin and Ethereum use the same cryptographic techniques to secure secure transactions, but can now also serve as a tool to protect against security attacks and security threats.

The advantages of blockchain in information security are mainly in the following four aspects:

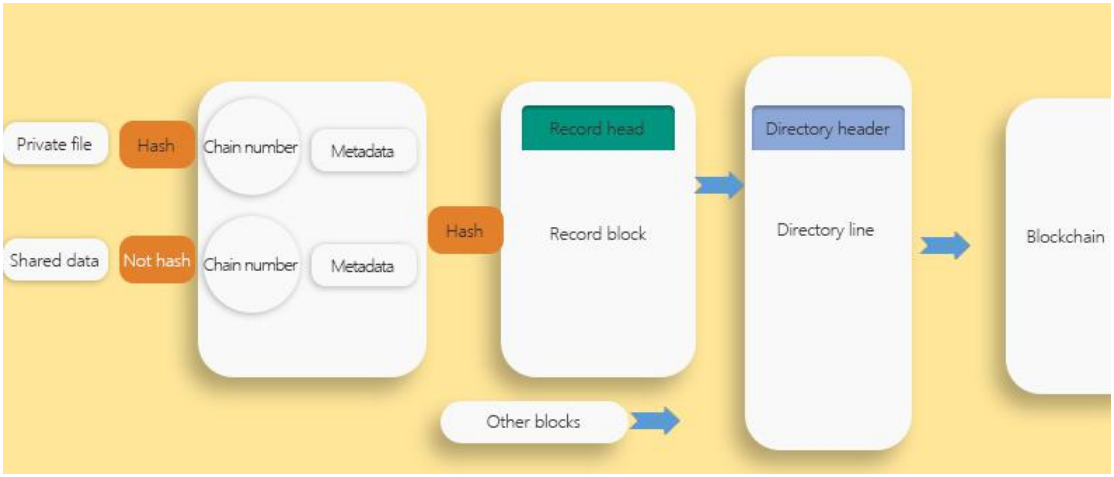
- Guarantee data integrity of information with highly redundant databases
- Use cryptography to verify data and ensure that it cannot be tampered with
- Rights management, using multiple private key rules for access control
- The transaction data on the blockchain is all accompanied by the digital signature of the trader and cannot be forged.





The use of blockchain security advantages allows for the development of multiple security applications. The existing security application scenarios are PKI, authentication, etc., and can be easily explained by two examples.

CertCoin developed by MIT may be the first PKI based on blockchain. PKI is a common form of public key cryptography that can be used to protect mail, messaging applications, websites and other forms of communication. However, since most PKI interfaces need to be centralized, trusted third-party certification authorities (CAs) issue, revoke, and save key pairs for each participant, and hackers can gain access to encrypted communications by impersonating users. . CertCoin removed the centralized authority and used the blockchain as a distributed ledger to distribute the public key, which can effectively reduce the risk of hackers' single point of intrusion.



Process diagram

In the field of certification, there are also many examples, such as the Gong Zheng Tong Factom system. It builds a chain structure based on the blockchain and decomposes the certification into three parts: the existence certificate, the process certificate and the auditable certificate. For the authentication of any digital asset, you can follow these three steps to achieve data record security and regulatory compliance.

6.1.2 KOK Pass Security Protection Application

6.1.2.1 Protecting border device security with authentication

Just as IT is concerned with the migration of data and connectivity to "smart" border devices, security is also concerned about this shift. After all, network expansion can increase IT efficiency, productivity, and power consumption, but it also poses security challenges for CISOs, CIOs, and the entire company. Many companies are therefore looking to apply blockchains to protect IoT and industrial IoT (IIoT) device security – because blockchain technology enhances authentication, improves data traceability and mobility, and aids record management.

6.1.2.2 Improve confidentiality and data integrity

Although the blockchain was originally created without specific access control mechanisms (derived from its publicly distributed attributes), some blockchain implementations are now addressing data confidentiality and access control issues. In today's era of data tampering or forgery, ensuring data confidentiality and integrity is a

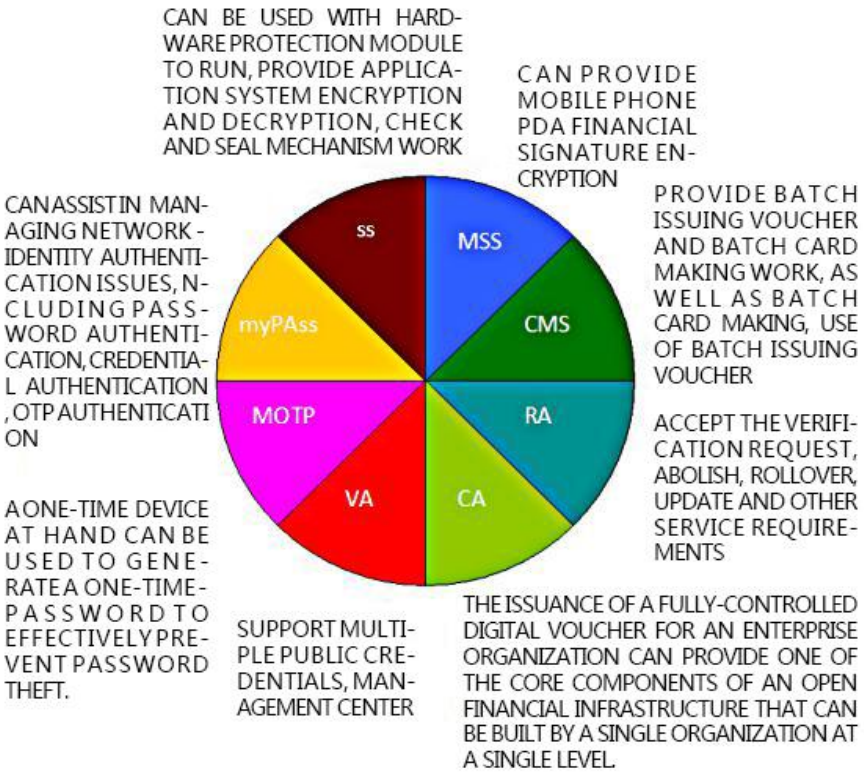
huge challenge. But the full encryption of the blockchain data ensures that the data is not caught by unauthorized parties, but it is still liquid (the possibility of a man-in-the-middle attack is almost unsuccessful).

This data integrity has also been extended to IoT and IIoT. For example, IBM offers the option to manage IoT data in a private blockchain on its WKOKson IoT platform, which is integrated into IBM's cloud services. Ericsson's blockchain data integrity service provides fully auditable, compliant and trusted data for App developers working on GE's Predix PaaS platform.

6.1.2.3 Protection of privacy messages

KOK Pass is using blockchain to protect live chat tools and private information circulating on social media. Unlike end-to-end encryption used by apps like WhKOKsApp and iMessage, KOK Pass uses blockchain to protect user metadata. Because the metadata is randomly distributed in the book, there is no single collection point, so it will not be hacked.

6.1.2.4KOK Pass promotes or even replaces PKI

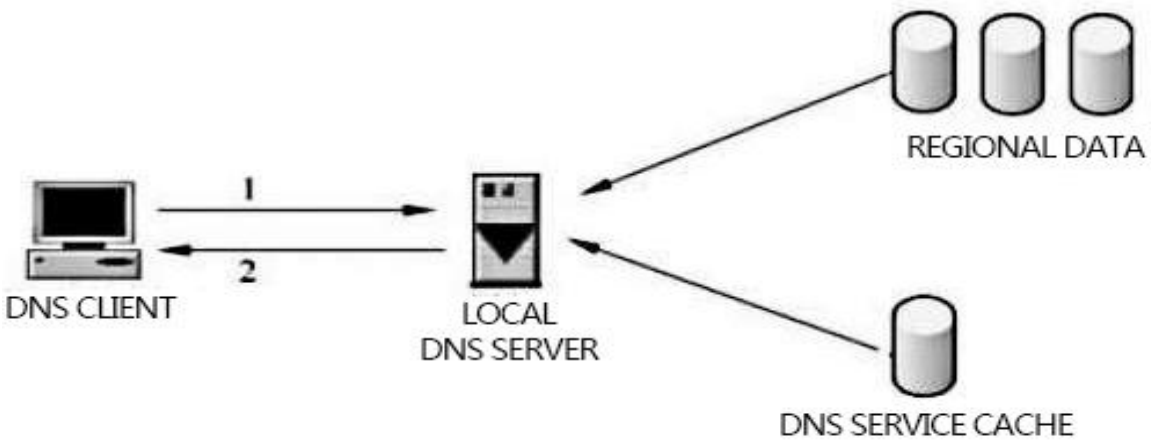


Public Key Infrastructure (PKI) is a public key cryptosystem that protects email, messaging applications, websites, and other forms of communication. However, most PKI implementations rely on centralized third-party certification authorities (CAs) to issue, revoke, and store key pairs, leaving cybercriminals with the opportunity to snoop on encrypted communications and fake identities. The issue of a key on the blockchain theoretically eliminates false key propagation and allows the application to verify the identity of the communicating object.

The KOK Pass is the first PKI implementation based on blockchain. The project as a whole abandoned the central certification authority and used the blockchain as a distribution book for the domain name and its public key. In addition, the KOK Pass provides an auditable public PKI without a single point of failure.

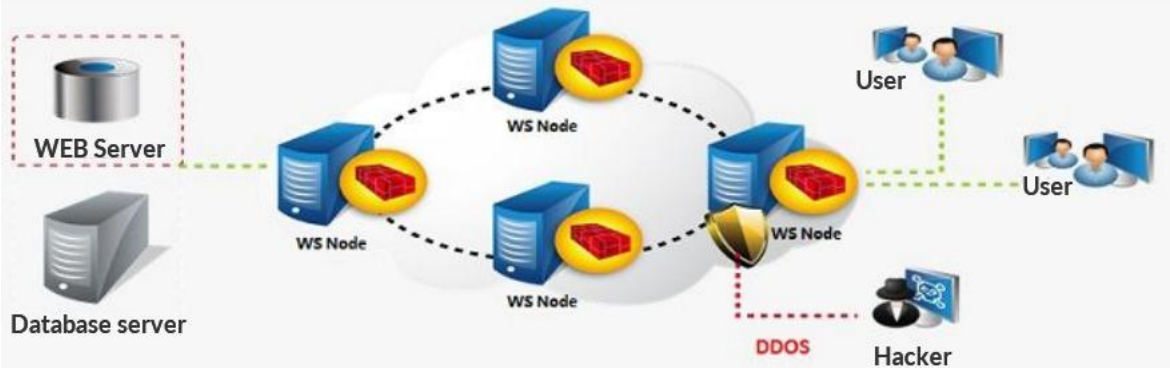
With KOK Pass Blockchain technology, we can sign transactions with citizen-generated identities.

6.1.2.5 More secure DNS



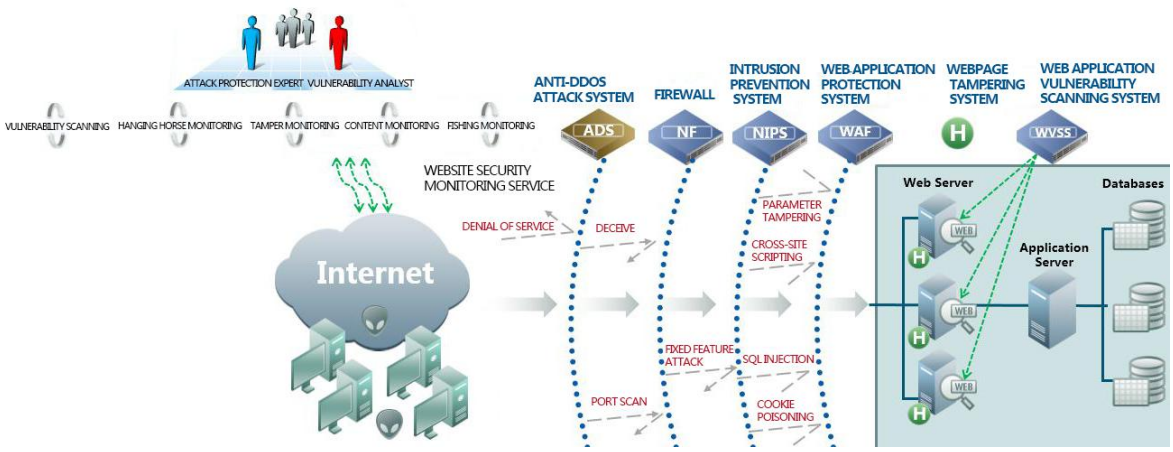
KOK Pass is a new project to explore the concept of distributed DNS. In theory, distributed DNS can cope with access request floods and will not crash due to overload of response. The KOK Pass uses the Blockchain 3.0 Public Chain and Interstellar File System (IPFS), as well as the HTTP Distributed Alternative Protocol, to register and resolve domain names. Internet-critical services such as DNS can be exploited by hackers to create large-scale dropped calls and attacks on corporate enterprises, so the trusted DNS infrastructure using the blockchain approach will greatly enhance the Internet core trust infrastructure.

6.1.2.6 Reduce DDoS attacks



6.1.3 Network Access Control

The KOK Pass public chain allows nodes to enter and leave the network freely, and the network layer of the blockchain does not have a registered user identity. The risk and security of the financial industry is relatively higher, and the unregistered nodes freely enter and leave the network to bring a lot of uncontrollability to the system security. When applying the KOK Pass blockchain technology in the financial industry, it should analyze the necessary use of the public chain and register the identity of the nodes in the network in combination with business needs. In addition, VPN private networks, firewalls, physical isolation and other technologies should be used to protect nodes, especially the physical network and hosts of miners.



6.1.4 Layer security

Mainly reflected in the following aspects:

The basic attributes that a consensus agreement should have: The KOK Pass blockchain uses a distributed consensus protocol to prevent single-point failures and other issues, effectively preventing double-cost, miners maliciously blocking a user's transactions and other attacks. However, this is based on the fact that the rights of the blockchain network nodes are evenly distributed and there is no 51% attack. Much depends on the consistency of the blockchain is not destroyed. Therefore, designing a suitable consensus algorithm is critical to the security of blockchain applications.

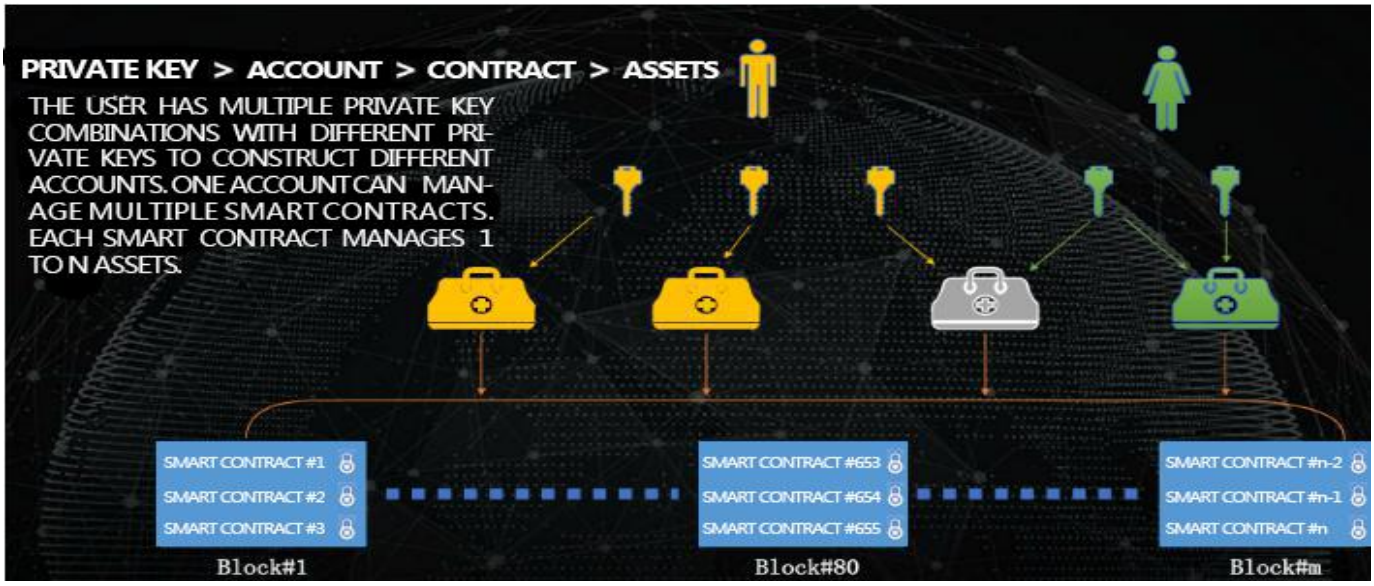
6.1.5KOK Pass Incentive Layer Security

The nodes in the KOK Pass blockchain are anonymous, and users do not need to register their true identity when using the system.

6.1.6 Smart Contract Layer Security

The intelligent contract layer was introduced in the Blockchain 2.0 release, and the concept of Blockchain as a Service (BaaS) was proposed. The smart contract layer provides a smart contract of automated script code to develop applications and manipulate data.

The smart contract is still essentially a programming language. If it is Turing-complete and supports looping instructions, an attacker could construct a transaction with an infinite loop code to launch a DoS attack on the miners in the network.



6.2 KOK Pass Wallet Security

KOK Pass Wallet has a major responsibility in protecting users' digital assets. Enhancing the security of hot wallets is the primary task of KOK Pass Wallet;

Enhance the security of hot wallets, increase the amount of hot wallet deposits, reduce frequent capital transfers between hot and cold wallets, enhance support for daily business, and improve operational convenience;

The KOK Pass Wallet uses a software-based hot wallet and cold wallet solution. It also introduces hardware-encrypted wallet management, directly generates hardware secret keys, double encryption, and protects digital assets.

6.2.1 KOK Pass Wallet Classification

By platform	By support currency	Divided by private key storage
Mobile end	Support for a single currency	Stored in the terminal device
PC side	Support diverse currencies	Stored in a hardware chip
		Stored on paper, etc.

6.2.2 KOK Pass Wallet Function

The most basic features of the KOK Pass Wallet include:

- Private key generation and management
- Generation and management of mnemonics

- Wallet address generation
- Support import of private keys and mnemonics generated by other wallets
- Transferring digital assets, etc.

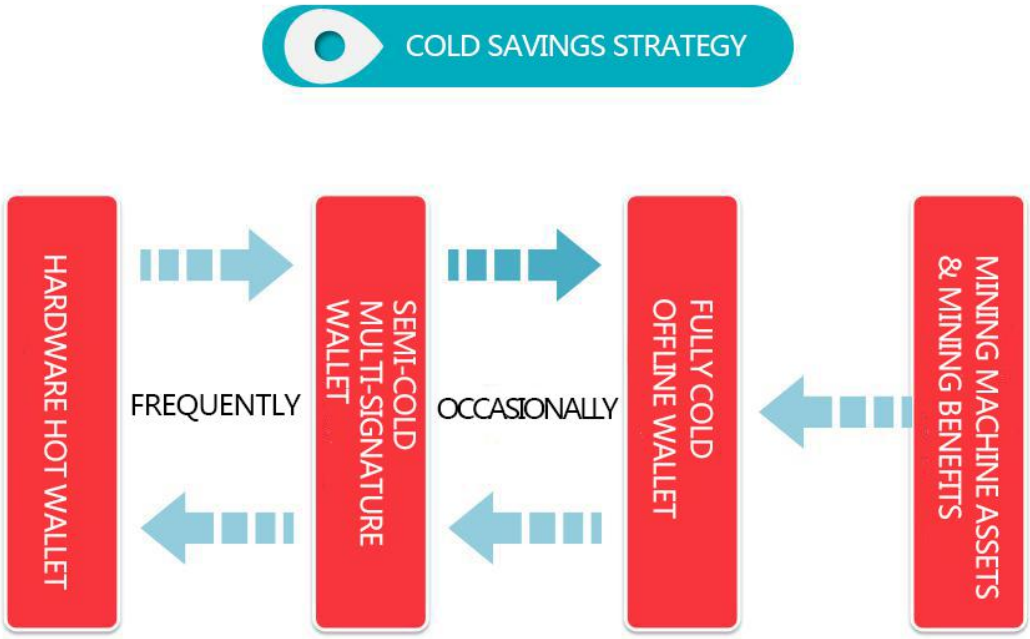
6.2.3 Security of KOK Pass Network Transmission

The security of network transmission is more reflected in whether there is a good ability to fight against man-in-the-middle attacks. Man-in-the-middle KOKtack (MITM) means that the attacker and the two ends of the communication create separate contacts and exchange the data they receive so that both ends of the communication think they are Direct dialogue with the other party through a private connection, but in fact the entire session is completely controlled by the attacker.

A secure digital wallet needs to be able to scan the legitimacy of all digital certificates in the terminal, check the proxy settings during network transmission, and ensure the security of the underlying network communication environment.

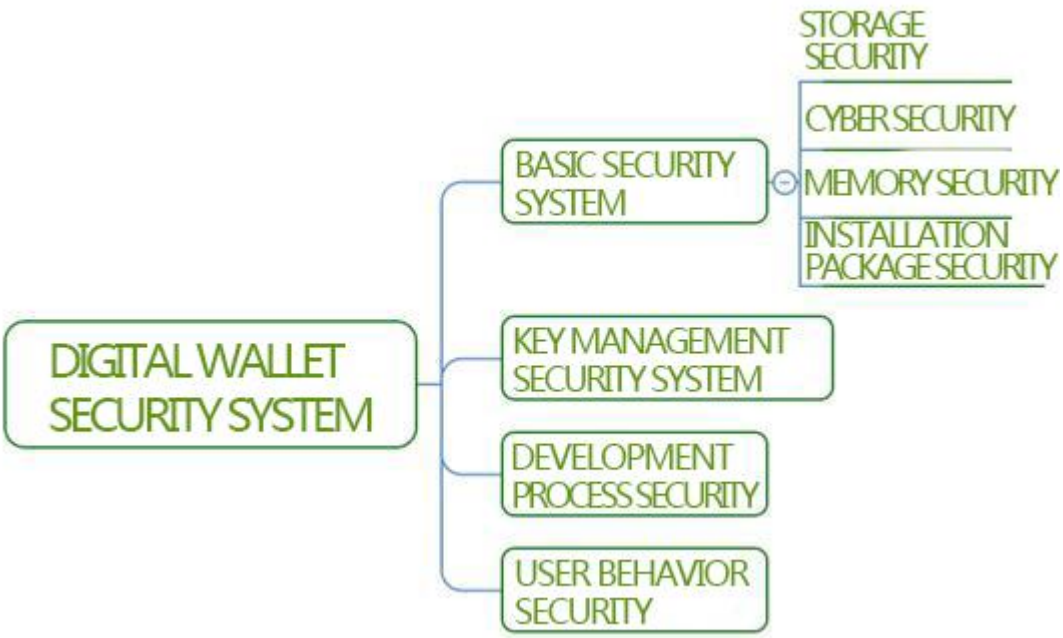
6.2.4 File storage security

For the private key/mnemonic of the digital wallet, the storage method of the terminal device also needs to pay attention to the security design. The access rights to the private key/mnemonic file storage directory, the form of the private key/mnemonic storage, and the design of the encryption algorithm all need to be carefully designed.



6.2.5 Safety standards for KOK Pass wallets

The KOK Pass wallet is designed to follow the following security systems: the underlying security system, the key management security system, the development process security system, and the user behavior security system.

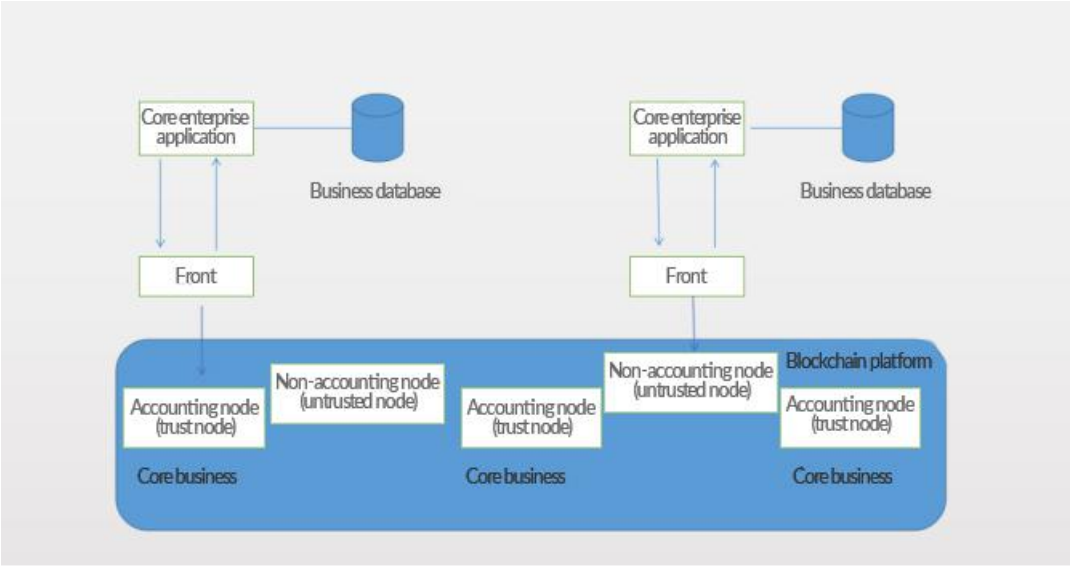


6.3 KOK Pass and Distributed Network

6.3.1 The nature of the blockchain

What is the nature of the blockchain? In fact, it is a distributed database.

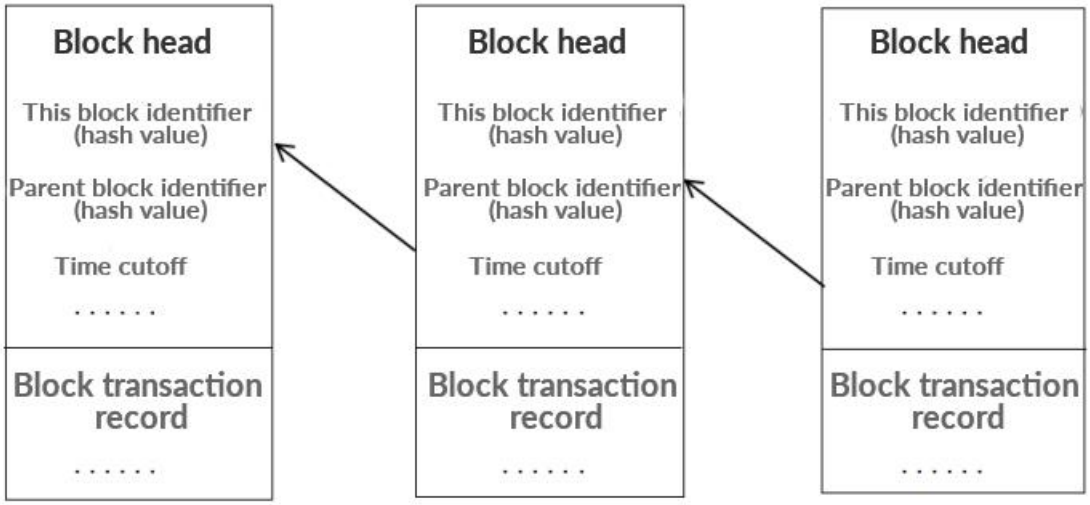
The commercial value of the application blockchain technology is more suitable for the blockchain technology in the multi-participation scenario. It also mentions the technical characteristics of the blockchain (1) multiple copies, (2) reliable records, and (3) non-tamperable (4) Several characteristics of multi-party transparency. The above characteristics are summarized. After using the blockchain technology, the application technology architecture is shown in the following figure. It can be seen that the blockchain technology is a distributed database for applications. One by one:



6.3.2 Distributed Data Storage

The data sharing of blockchain technology is a distributed accounting book with multiple copies of transaction records, so the problem of distributed data storage must first be solved.

The basic unit of blockchain storage is a block, and the block adopts a chain structure, that is, the newly added block (like a row of a database record) knows what its previous block (the previous row record) is, and can be traced back to the root. The identifier of the block is the hash value of the block, and the chain structure retains the trajectory generated by the service, and can be verified according to the previous record when the transaction is newly added, thereby ensuring that the content of the block is not easily falsified.

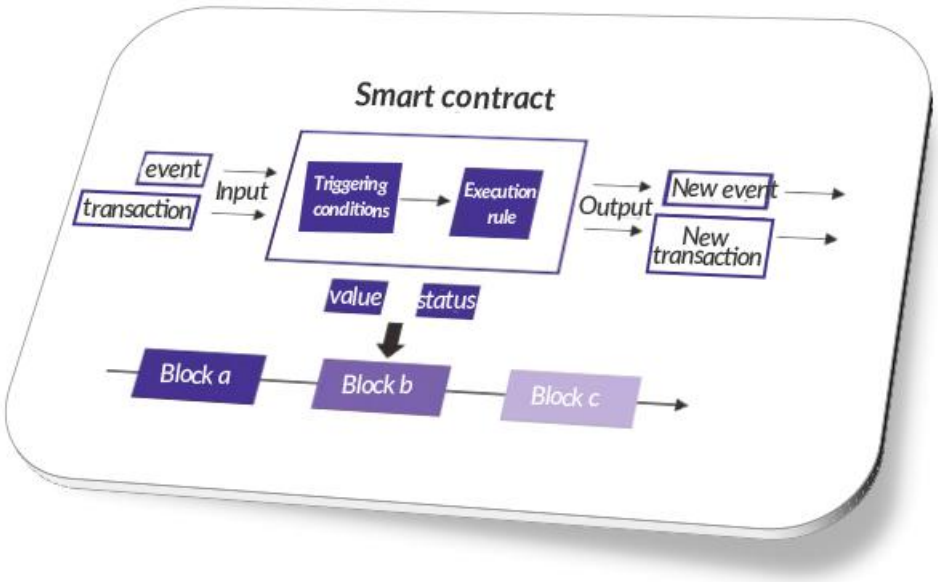


6.3.3 Point-to-point reliable transmission

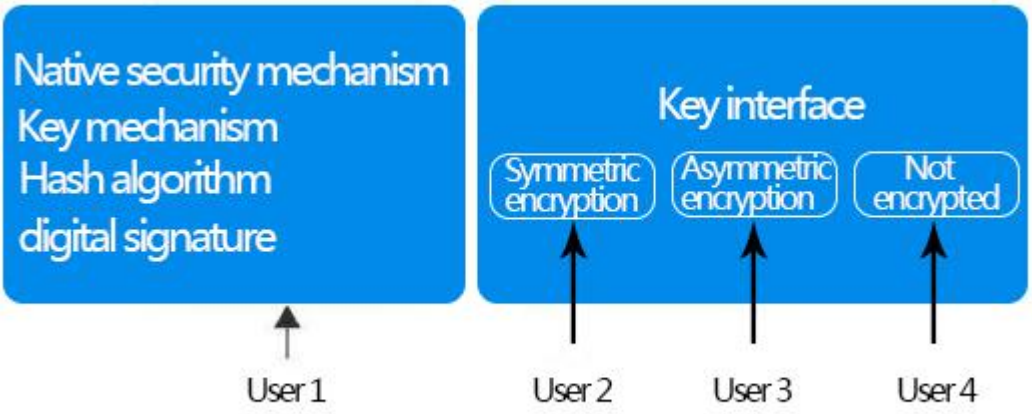
6.3.4 Smart Contracts: Triggers and Stored Procedures

A smart contract is a digital contract that can be automatically executed when certain conditions are met. Implementing this feature is done in the database by triggers and stored procedures. Although in the current popular application architecture, it is not recommended to write logic in the stored procedure, but triggers and stored procedures are still commonly used tools, especially in the operation and maintenance activities related to

data migration. The smart contract in blockchain technology is the trigger and stored procedure. It is a script that runs in the sandbox and is used to execute the business logic in the blockchain business. It can also be used for various checks.



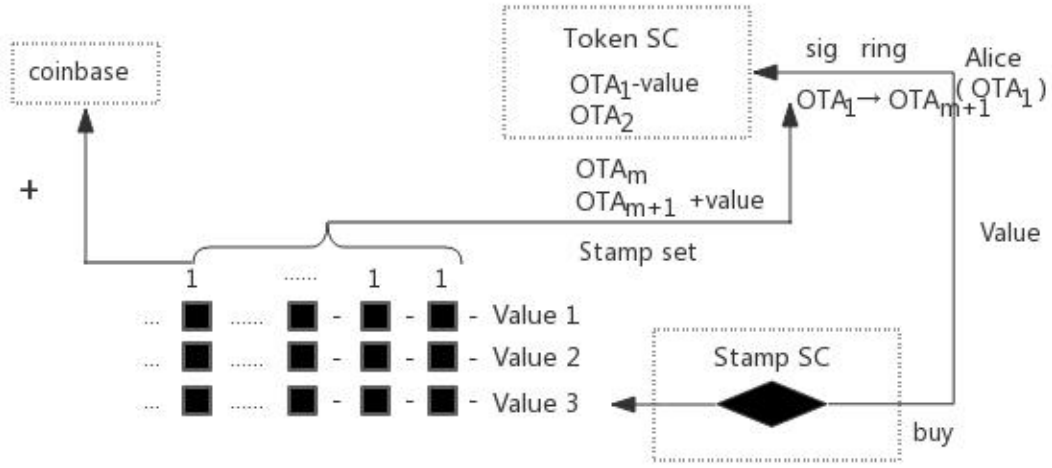
6.3.5KOK Pass Data Security



chapter VII KOK Pass Privacy Protection Effect

7.1 KOK Pass Trading Privacy Protection Plan

- 7.1.1 Trading scenario
- User 1 primary address private key is (a, b), primary address public key is (A, B); user 2 primary address private key is (c, d), primary address public key is C, D. User 1 has the address OnKOKime − account1 in the smart contract SC, and wants to transfer the value currency for User 2 from this address. This is the scene of the transaction.
- 7.1.2 Trading Process
- transaction initiation
- Transaction initiation process
- transaction verification
- Transaction verification process
- transaction confirmation
- Transaction confirmation process



7.1.3 Analysis of privacy effects

The privacy policy based on OnKOKime-account and ring signature can achieve the following privacy effects:

1) Use the stamp system and ring signature scheme to ensure that the originator of the transaction is anonymous throughout the network.

2) Use OnKOKime-address to ensure that the smart contract currency address is isolated from the primary address.

7.2 KOK Pass Signature Scheme

7.2.1 Group signature general process:

1) Initialization

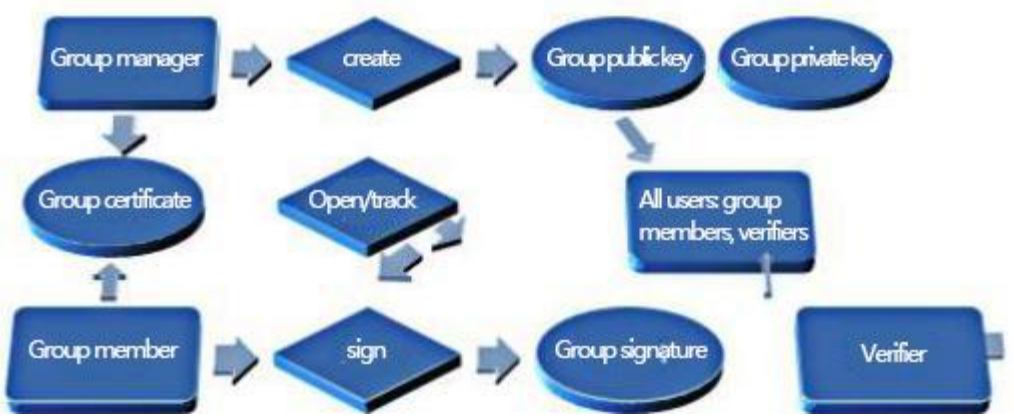
2) Member join

3) Signature

4) Verification

5) Open

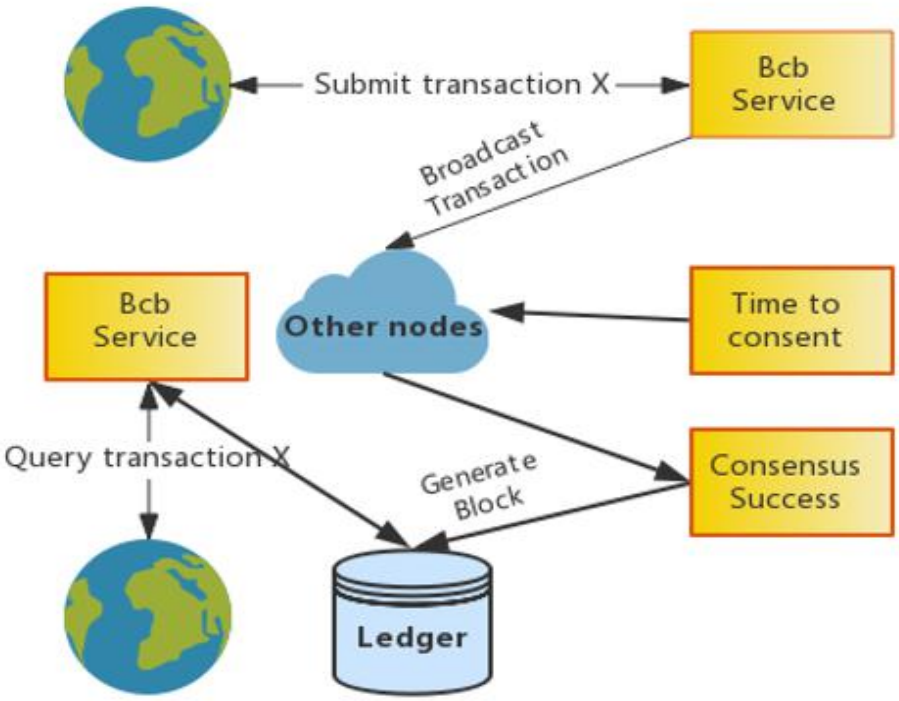
7.2.2 Research future:



Chapter VIII KOK Pass Technical Features and Advantages

hrough a large number of business models, application model data test analysis, KOK pass blockchain can achieve performance: second-level transaction verification, massive data storage, high throughput, fast synchronization of node data; can be achieved in terms of scalability: meet more Business block structure, access control policy; at the same time, provide secure private key access services, and privacy protection solutions.

8.1 Performance aspects



1 fast transaction verification

Through the optimization of key algorithms such as signature algorithm, account structure, data operation, serialization, consensus mechanism, and message diffusion, the KOK Pass blockchain can achieve fast transaction verification in seconds. Meet the user experience of most blockchain application scenarios.

2 massive data storage

The blockchain double-entry bookkeeping mode, the historical data is accumulated under the long-term operation of the system; the KOK Pass blockchain borrows the mechanism of separate storage and storage of hot and cold data in the traditional financial system to realize the effective storage of massive data. Old transaction data, inactive asset data and other information can be stored using a big data storage platform (such as Hadoop, which meets PB level data storage).

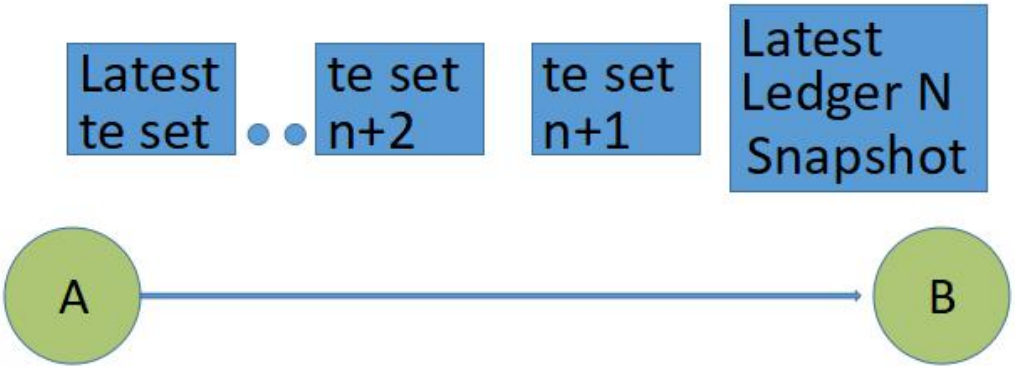
3 high throughput

The essence of the blockchain is a distributed shared accounting technology, and its distributed features are mainly reflected in distributed consistency rather than distributed concurrent processing. In order to ensure data consistency and prevent the Byzantine general problem, certain specific links can only be executed serially, but not in parallel. Through long-term testing and optimization practices, the processing performance of the KOK Pass Blockchain has been able to meet the needs of the 10,000-level TPS. If you introduce a mechanism such as Off-Chain, you can further increase the transaction throughput.

Fast synchronization of 4-node data

The KOK Pass blockchain supports the Snapshot mechanism, which can periodically mirror the local ledger and

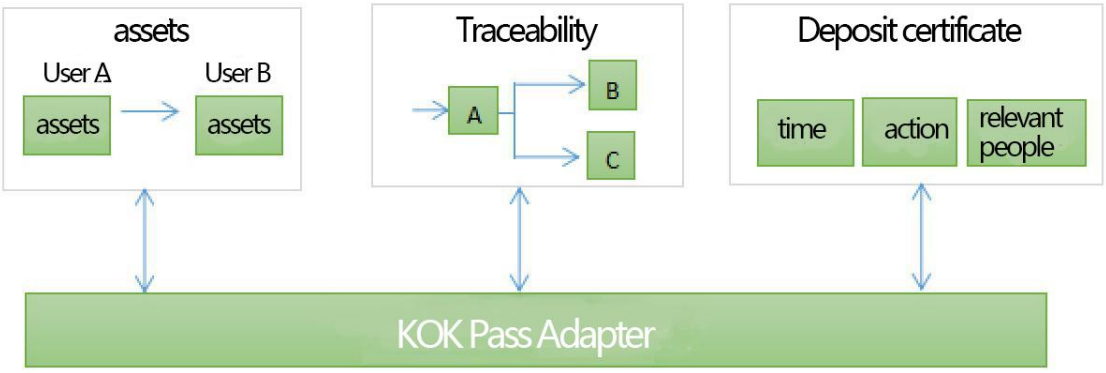
implement a convenient rollback mechanism. Under the unified consensus, you can specify the mirrored label to roll back. At the same time, shorten the period during which the newly added node joins the operation. Just sync the latest image and a small number of recent transaction collections to integrate into the network and participate in consensus verification.



8.2 Aspects of scalability

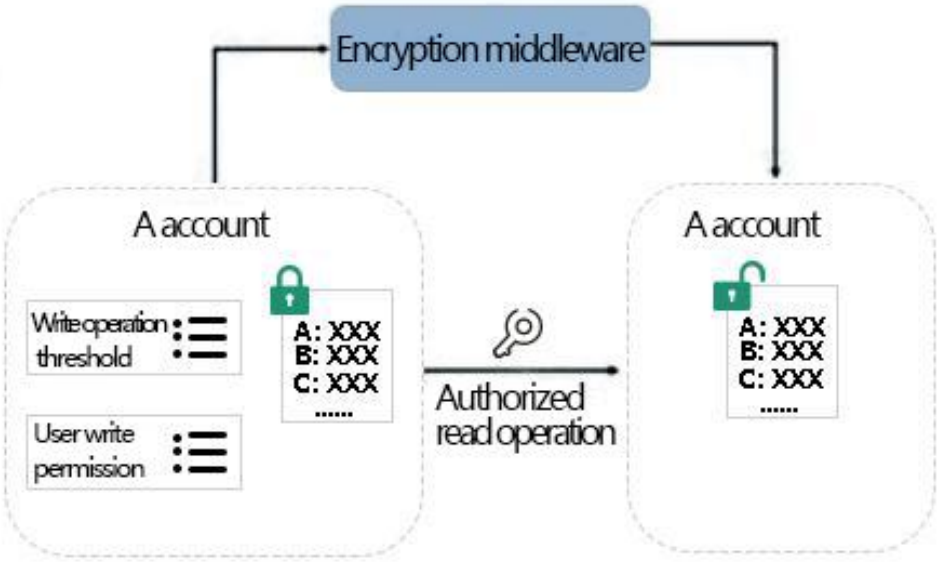
1 to meet the multi-service blockchain structure

The blockchain structure of the KOK Pass blockchain can meet the needs of different business areas and improve the system's scalability and maintenance efficiency. It can be used to tag assets and asset transfers, as well as provide multi-dimensional event records that cannot be tampered with, and can also be used to trace sources to track the flow of items.



2 permission control strategy

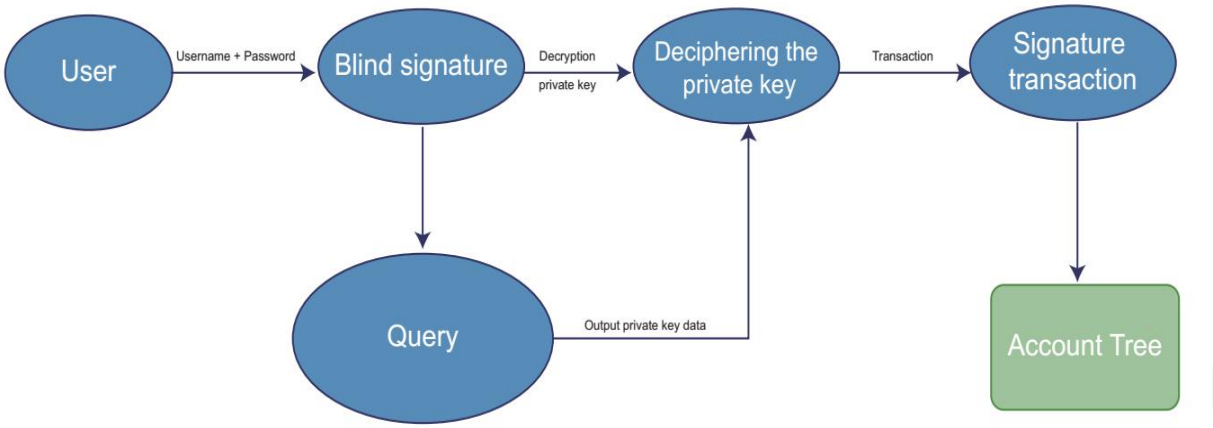
Provide two types of permission control policies for data information writing and reading. Data information write permission, multiple users are set under the same account, and corresponding permissions are set for different operations to satisfy the usage scenario of multi-party signature control. The data information read permission allows the user to grant and withdraw the operation rights of the single user or user group to the data. The user group can be flexibly configured by the user. The data includes user account information, transaction information, etc., and the granularity can be refined to the attribute fields of the transaction or account.



8.3 Security aspects

1 secure private key access

In order to facilitate the user to use the blockchain product service, in addition to the traditional client generation and storage mechanism, the KOK Pass provides both network escrow access and private key hardware access (U-key). Web-managed access, that is, mapping a username and password to a private key through a specific algorithm and storing it on the server. The private key stored on the server side is encrypted data, and the private key can only be decrypted at the user end; the hardware private key is to meet the needs of the financial industry and the Internet of Things industry.



2 multiple privacy protection scheme

Provide multiple privacy protection features. First, the bottom layer of the blockchain provides a homomorphic encryption method, and all data of the user is encrypted and stored, and only the user itself is visible. Secondly, KOK provides an encryption middleware service that users can choose based on business needs. Finally, the upper application can encrypt the data when it is entered, and the KOK platform is responsible for writing and reading the encrypted data generated by the user.

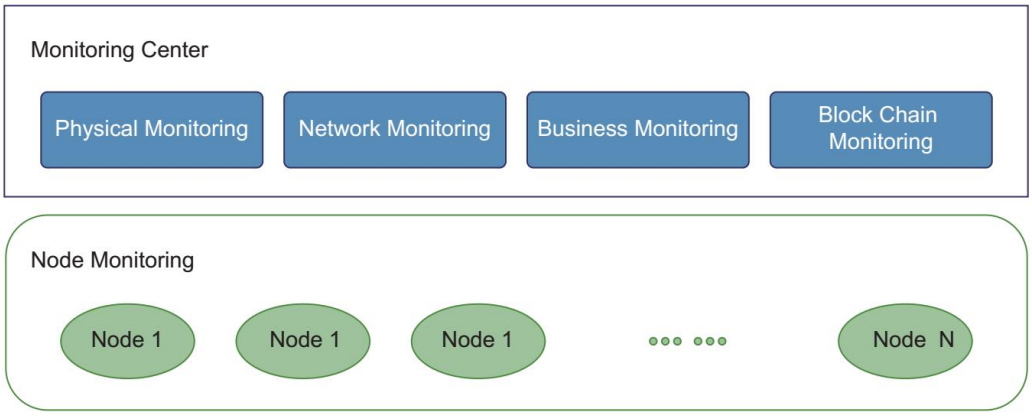
8.4 Operation and maintenance aspects

1 full platform deployment

All code of the KOK Pass blockchain can be compiled and run across platforms. The platform-related code is packaged into a base library, and the business logic is independent of the KOK Passport platform. In addition to PC and server mode compilation, it also supports cross-compilation methods, such as ARM and MIPS platforms, which facilitates deployment in mobile portable systems and provides preliminary support for blockchain Internet of Things. At the same time, the KOK Pass has reached strategic cooperation with several well-known cloud platforms in China, enabling rapid deployment on the cloud platform.

2 visual operation and maintenance

Provides the visualization tools needed for operation and maintenance management. System monitoring services deployed on blockchain nodes (MonitorAgent): Supports data (block, transaction, contract, consensus, etc.), network (networking, delay, throughput, etc.), system level (CPU, memory, disk, etc.) data information monitoring; Logs, alarms, and notification mechanisms facilitate the maintenance of commercial systems.



3 low-cost access method

BubiAdaptors abstracts API interfaces for a variety of business scenarios, such as assets, traceability, deposit certificates, etc., for direct use by services related to these scenarios. In the new business scenario, the KOK Pass can quickly customize the interface to meet the business function requirements based on the existing framework. It also provides packaged SDK software development packages that support a variety of mainstream development languages (JAVA, C++, node-js, PHP).

At present, there are two main types of blockchain technology services: one is to build a set of blockchain bottom layer, provide a standardized API and open, and then the developer can dock the application itself; the other is to solve some industry pain points with the upper application. , the distributed ledger is embedded in the existing application system. Blockchain is an emerging technology. Only by continuously meeting the needs of the business can we mature. Therefore, we reduce the threshold of the upper-layer application by encapsulating the underlying distributed ledger, and continuously optimize and optimize the process of docking and use. Improve the underlying distributed ledger and consensus algorithms to make them more relevant to commercial appeals.

Chapter IX Technical Solutions for KOK Passes

9.1 Consensus mechanism

The essence of the consensus mechanism is a fault-tolerant algorithm used to solve the problem of data consistency in the Byzantine network. It is generally called the Byzantine fault-tolerant distributed consistency algorithm. At present, there are four types of consensus mechanisms in the mainstream of blockchain: workload proof mechanism (Proof of Work, POW); Proof of Stake (POS); Authorized Equity Proof Mechanism (DPOS); and Practical Byzantine Agreement (PBFT).

POW relies on machines to perform mathematical operations to obtain billing rights. Resource consumption is higher than other consensus mechanisms and can be weakly regulated. At the same time, each time a consensus is reached, the entire network needs to participate in the operation, the performance efficiency is relatively low, and the fault tolerance allows the whole network. 50% node error.

There are many different variants of the POS equity certification mechanism, but the basic concept is that the difficulty of generating a block should be proportional to the share of the user in the network. This method does not consume energy.

The DPOS representation system is similar to the board vote. The holders vote for a certain number of voting nodes and represent them for verification and accounting. This approach significantly reduces the number of participating verification and billing nodes and speeds up transaction confirmation.

PBFT is a message-based consistency algorithm. The algorithm achieves consistency through three stages. These stages may be repeated due to failure. The algorithm is mainly applied in the alliance blockchain or private

blockchain scenario.

The above four types of consensus mechanisms are applied in different application scenarios, and currently have better applications. There is still a class called hybrid mechanism, and the developers of the blockchain adopt the "POW+POS" approach to combine the two, and the advantages and disadvantages are complementary.

The KOK Block Chain Pass will be developed according to its own industry. It will combine the Paxos algorithm and some excellent algorithms to develop a consensus mechanism that is more suitable for agricultural products, shorten the verification time, improve the transaction confirmation speed, and improve credit. Data query efficiency in the system 9.2 Multi-chain system.

In the early days, a two-way peg sidechain solution made an effort to expand the scalability of Bitcoin. Later, the rise of platforms such as Ethereum provided more possibilities for scenarios and ways of cross-chain interaction. So born, there are some sophisticated items like

BTC enables Ethereum DApp developers to make API calls from smart contracts to BTC Relay to verify Bitcoin network activity; there are also projects dedicated to implementing "InternKOK of BlockCHAINs", such as Cosmos and Polkadot, through

Hub/relay implements chain value transfer/global consensus. To date, most cross-chain interoperability efforts have remained in experimental scenarios or are limited to the public chain. The latter is related to the lack of development maturity of the alliance chain and lacks the soil for exploration and testing.

The KOK Block Chain Pass (KOK Block Chain Pass Card) adopts a mesh multi-chain system and consists of three sub-chains: identity chain, data link and payment chain. The identity chain is used to record the information of the credit subject in order to authenticate and credit the credit subject; the data link is mainly used to record the transaction of the credit subject and the product data; the payment chain is mainly used to carry the Token of the Chinese Dragon Chain.

This design can meet a variety of needs, including the core enterprise, upstream and downstream small and micro enterprises, government, universities and supply chain financial institutions, as well as ordinary individual users. For small and micro enterprise entities, the identity chain and data link are its credit scenarios; for financial institutions or ordinary users, they only need to pay attention to the payment chain. Different sub-chains maintain the same consensus algorithm and implement concurrent transactions to improve overall transaction efficiency.

9.3 Privacy protection

Due to the security of the data, the KOK Block Chain Pass has been improved in many aspects to support and be compatible with all RFID-based, NFC-based IoT data acquisition devices currently on the market. The data can be transferred to the KOK Block Chain Pass (KOK Block Chain Pass) network and track the flow of items in the KOK Block Chain Pass Card network. The IoT device collects data, and the KOK Block Chain Pass network collects data from the device through the API interface.

Since the data recorded by the blockchain involves enterprise transactions and product data, the

financial institution needs to obtain the authorization of the subject to be inquired before the inquiry, which is the privacy protection of the data subject. Only through two-way authentication can the data of the credit subject in the KOK Pass be queried for each identity. Only the query key can be used to view the information related to the transaction of the data subject in the supply chain and the information of its products. .

The homomorphic encryption technology is adopted in the blockchain, and the homomorphic encryption technology stores the information of the data subject in the supply chain and the information of the product in the blockchain to achieve a perfect balance, and will not be a block. The chain attribute causes any major changes. In other words, the blockchain is still a public blockchain. However, the data on the blockchain will be encrypted, thus taking care of the privacy of the public blockchain, which allows the public blockchain to have the privacy effect of a private blockchain.

9.4 Data Storage

As enterprise entities increasingly access blockchains and the frequency of corporate transactions increases, corporate transaction data and project data storage will gradually increase. The application of blockchains in different supply chain scenarios will also result in a significant increase in data. In order to ensure that data storage does not affect payment and authentication, the first is to use the data link and the identity chain and the payment chain to separate the data structure design. The second is to use more light when more and more enterprise entities access the software. The client (Simplified InformKOKion VerificKOKion) method to verify the true reliability of the information, which greatly reduces unnecessary resources and storage space in the verification and transaction, and lays a foundation for mobile operations.

9.5 Identity and Access Mechanism

The KOK Block Chain Pass uses the industry-recommended digital certificate mechanism for identity authentication and access control. The third-party trusted authority, the Certificate Authority (CertificKOKe Authority), binds the public key of the organization to other identification information of the organization and can be used to verify the identity of the user on the network. KOK Block Chain Pass Card The mechanism and process for implementing identity authentication between alliance chain nodes using CA certificates are as follows:

1. The organization submits its own organization basic information (name, organization number, contact information, etc.), its node information (IP address, node identifier, etc.) and CA public key certificate to the chain operation manager for unified access audit.

2. If the institutional access audit is passed. The alliance chain operation administrator broadcasts the node information of the organization, the CA public key certificate to the entire alliance chain, and informs all participants; the new node of the new organization is connected to the network, and the active node in the chain should allow the new node to connect. And shaking hands.

3. When the nodes are connected to each other, the nodes will use their private key in the CA certificate to sign their handshake information and send it to the other party. The receiver queries the CA public key

certificate according to the sender's handshake information and uses the public key certificate. Signature verification is performed to determine which organization's node initiated the connection and whether to allow communication to continue.

4. The certificate management service will periodically check the certificate status of the organization and determine whether the certificate is valid, such as whether it has expired or been revoked. If the certificate has expired, the node of the organization will be rejected when it tries to connect to the network.

9.6 KOK Block Chain Pass Card KOK Pass Traceability Platform

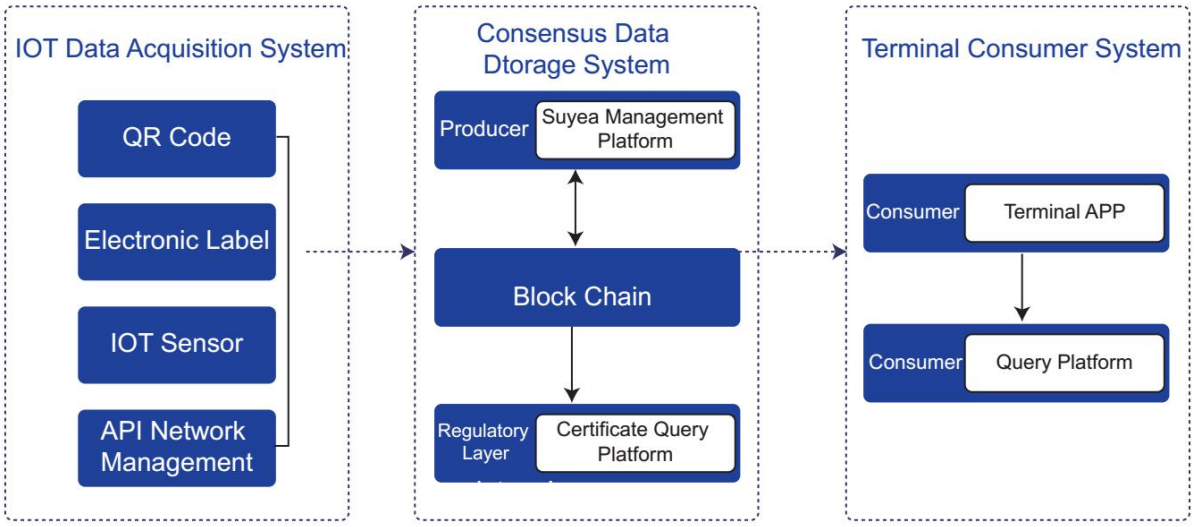
The KOK Block Chain Pass Card product traceability platform based on blockchain technology is the ecosystem of the KOK Pass industry. The overall ecosystem includes the following parts:

IOT data collection system The core value of the IOT system is that it automatically collects process data and uploads it to the blockchain platform during the production process. There is no need for manual intervention to achieve unique and credible data.

Consensus data processing and storage system uses the blockchain public chain as the underlying self-developed blockchain platform to classify and store the data collected by IOT devices, in which the consensus data is stored in the blockchain; pictures and product data storage in

In the IPFS distributed storage, the Ethereum Merkel tree storage solution was introduced.

The terminal consumer system is the user-oriented link in the HALAL product. This platform includes the verification platform for the traceability of the KOK Pass product, and realizes the function of the end consumer to query the traceability information of the purchased product.



Chapter 10 KOK Block Chain Pass Card Business Application Scenario

10.1 Supply Chain Management

➢Supply Chain Finance

In the traditional supply chain finance field, the trust endorsement of the core enterprises only supports the first-tier suppliers or the first-tier dealers, and cannot be extended to the second-tier and third-tier suppliers. Because the absolute superiority of the core enterprises often leads to the secondary and tertiary supply. There is a large financing need for the business. Based on the KOK blockchain supply chain finance, the core enterprise trust endorsement can be passed to the second, third or even more level suppliers, so that the ecological chain system surrounding the core enterprise can develop healthily. At the same time, for financial institutions, it is also possible to play back the historical data of relevant suppliers as a node method, reduce financial risks and enhance financial trust.

➢Supply chain settlement

For traditional double-entry bookkeeping, the biggest problem is the liquidation process of the supply chain. Based on the KOK Pass Blockchain solution, it can revolve around the multiple suppliers of the core enterprise. When the transaction is completed, the transaction signature information confirmed by the supplier and the core enterprise is synchronized on the blockchain to make the relevant transaction records. No tampering can be done. Efficient supply chain clearing services such as clearing, token settlement, etc.

10.2 Depositary field

As we all know, blockchain has high security and non-tamperability characteristics, so it can be applied to various high-security depository occasions, such as court confession, suicide note, contract terms, student record, and art deposit. The blockchain itself does not solve the one-to-one correspondence problem between the information source and the information body in the field of deposit verification. In this respect, the information representing the traditional data can be sampled through the existing Internet of Things RFID radio frequency technology, artificial intelligence technology or biometric identification technology. The object of the asset of the blockchain. The deposit information can be used for direct verification or for indirect verification. For example, a sample data representing the value can be used to determine the reliability of the sample data through the blockchain, and then the technical analysis of the information to be verified is confirmed.

10.3 Traceability field

The KOK blockchain can be applied to the traceability field of various items, mainly adopting the "chain" characteristics of the blockchain. Traceability areas include food traceability, product traceability, luxury traceability, and jewellery and jade traceability. The asset code representing the physical asset is circulated in all links of the blockchain, ensuring that the traceable information cannot be tampered with and can be traced completely. In the field of traceability, the KOK blockchain can add more customized traceability information (such as asset stories) to each traceability link through its own memo field to achieve asset value enhancement.

10.4 High security area

A blockchain is a value network composed of different organizations, different institutions, or individuals. Any individual revision of the book will not cause tampering with the data. The blockchain itself has a financial-level signature algorithm and uses distributed storage technology. In a certain sense, the blockchain has a higher security level than the existing financial system. Therefore, the blockchain is very suitable for military and financial fields with high security levels.

10.5 Self-reporting field

With the implementation of the real-name system model in the country, the establishment of a credible society has gradually increased the cost of untrustworthy individuals and institutions. However, most of the current credit information is in BKOK, which is difficult for large-scale SMEs or organizations to get involved with. Through the open access principle, KOK Pass supports each organization and individual to write the credit information of each person, and provides the whole society with credit information, which provides an industry standard for the establishment of self-collecting society.

10.6 Data Persistence

The blockchain is an infinitely increasing book structure. Any operation cannot affect the existing book data, and the book data is distributed in different organizations and different nodes. The larger the node size, the wider the information dispersion. Therefore, for any small-scale node failure or data corruption, the integrity of the data is not affected. Therefore, the data of the KOK Pass blockchain is more suitable for the "Vows", such as emotional deposit registration, promise deposit.

Chapter 11 Overview of the KOK Pass Issuance Plan

11.1KOK Pass Overview

The KOK Block Chain Pass is the proof of the rights of the Chinese currency trading platform itself and is the only global certificate. Have an innovative "transaction is mining" mechanism. The total amount of KOK issuance is 8.4 billion yuan and will never be issued. KOK will allocate most of the income to the holders of the Chinese currency in a timely manner. In addition, KOK holders share various rights such as community governance.

11.2 KOK Pass Trading Model

The “transaction-mining” model is gradually released to the user via the KOK form, and the released part enjoys the distribution of income. 45% of KOK will be awarded to community users through the “transaction-mining” model, 44% of KOKs are placed in the hands of participating users through crowdfunding, 5% are held by the founding team and pre-locked, and the remaining 6% are used Chinese currency Fund. These four parts of KOK are called “mining part” and “issuance part (crowdfunding total + initial team release total + Chinese currency fund)”.

The user obtains the “transaction-mining” mode, and returns a KOK period for one fee per day. The KOK quantity expected to be returned will be calculated according to the average price and distributed to the user in time.

44% of the total issuance is used for pre-locking of crowdfunding, and the liquidity generated by market liquidity and trading mining is released in proportion, and the released part enjoys platform income distribution. The 5% founding team holds, the liquidity and the liquidity generated by the transaction mining are released in proportion, and the released part enjoys the platform income distribution, but promises not to enter the market for circulation within one

year. There is also a 6% Huayuan Fund (fund) to support the Chinese currency ecosystem. That is: the current total circulation of KOK market = KOK/45% of accumulated mining output.

11.2 KOK Pass Allocation Scheme

1About KOK liquidity/participation income distribution ratio

45% of the total issuance: it is gradually released to the users through the mining method, and the released part enjoys the distribution of income. The KOK period is refunded once a day, and we will calculate the amount of KOK expected to be returned at the average price and distribute it to the user in a timely manner.

44% of the total issuance: it is released to the participating users through crowdfunding, and is pre-locked. The liquidity generated by the market liquidity and trading mining is released in proportion, and the released part enjoys the platform income distribution.

5% of the total issuance: held and pre-locked by the founding team through pre-issuance, the liquidity and the liquidity generated by the transaction mining are released in proportion, and the released part enjoys the platform income distribution, but promises within one year. Do not enter the market for circulation.

The remaining 6% is the Huayuan Fund that supports the Chinese currency ecosystem.

2About KOK income distribution mechanism

80% of the revenue of the China Dollar Digital Trading Platform will be allocated to KOK holders and 20% for the development and operation of the China Dollar trading platform. The platform's revenue includes, but is not limited to, the platform's fee income.

The principle of our distribution is: what is distributed, what is distributed, and distributed proportionally. For example, the fee income includes BTC, KOKH, LTC, KOK, etc., and the allocation is also BTC, KOKH, LTC, KOK, and so on.

Income distribution is based on a distribution period. For example; July 3, 2018 (GMT+8, the same below) is the first distribution date. Starting from the daily (GMT+8) 0 point, the transaction fee of 100% generated by the user is converted into KOK every hour and distributed to the KOK holder. The calculation of the total turnover of KOK is converted in association with BTC (depending on the turnover of all KOK trading pairs, associated with the BTC price). The return time of the fee is: the amount of the distribution generated on the hour of the day is returned to the hour of the next day.

3About KOK “transaction is mining” personal transaction fee refund mechanism

Overall, 45% of KOK is gradually fed back to trading users through “transactions, ie mining”. Once 45% of KOK is fully returned, “mining” is automatically terminated. The specific method of “transaction is mining” personal transaction fee refund mechanism is:

Starting from the daily (GMT+8, the same below) 0 points, the transaction fee generated by the user will be calculated every hour, and 100% will be converted into KOK for accumulation. The conversion price will be calculated according to the average price of KOK for the hour (the average price calculation method is Total transaction amount / total volume). Returned once per hour, returning the mining output in the same hour interval 24 hours ago. For example, in the interval of 7:00-8:00 on a certain day, the return of the previous day is from 7:00-8:00.

Chapter 12 Risk Warning

As a new investment model, digital asset investment has various risks. Potential investors need to carefully evaluate investment risk and their own risk tolerance:

12.1 Token Sales Market Risk

Because the token sales market environment is inseparable from the overall digital asset market situation, such as the overall market situation is low, or there are other uncontrollable factors, it may cause the digital assets themselves to have a good prospect, but the price is still undervalued for a long time. status. In addition, tokens are traded on the open market, often with price fluctuations. Such fluctuations may be caused by market forces (including speculative trading), regulatory policy changes, technological innovations, exchange availability, and other objective factors that also reflect changes in the balance of supply and demand. Regardless of whether there is a secondary market for KOK token transactions, the project party is not responsible for any KOK token transactions in the secondary market. Therefore, the risk involved in the KOK token transaction price is borne by the KOK token trader.

12.2 Regulatory risk

Due to the early development of the blockchain, most countries and regions around the world do not have relevant regulatory documents related to pre-requirements, transaction requirements, information disclosure requirements, and lock-in requirements in the crowdfunding process. It is still unclear how the implementation of national policies will be implemented. These factors may have an uncertain impact on the investment and liquidity of the project. Blockchain technology has become the main target of regulation in all major countries in the world. The existing regulatory approval or tolerance for KOK tokens or this public replacement in any country may be temporary. The Project Party may from time to time receive inquiries, notices, warnings, orders or rulings from one or more authorities, and may even be ordered to suspend or terminate any action regarding this public replacement, KOK token development. The development, marketing, promotion or other aspects of the KOK token and this public replacement may therefore be severely affected, hindered or terminated. At the same time, KOK tokens may be defined as virtual goods, digital assets or even securities or currencies at any time, so in some countries, KOK tokens may be prohibited from trading or holding in accordance with local regulatory requirements. In addition, procedures that are prohibited or restricted in certain jurisdictions, such as those involving gambling, betting, lottery, lottery, pornography, etc., may utilize the KOK Token Blockchain's non-access requirements to develop, promote, and market. Or operate. Regulatory authorities in specific jurisdictions may take appropriate administrative or judicial measures for specific procedures or even their developers or users. Any government authority's penalties, penalties, sanctions, repressions, or other regulatory measures may more or less scare or deter the existing or potential KOK token user using the KOK token system and holding the KOK token, thus the KOK token The prospects have a significant adverse impact.

12.3 Competitive risk

With the development of information technology and mobile Internet, digital assets represented by “bitcoin” are gradually emerging. Various centralized and decentralized digital asset exchanges continue to emerge, and

competition in the industry is becoming increasingly fierce. Although KOK tokens will quickly realize the flow of assets and the activity of the platform by injecting hundreds of millions of dollars of digital assets and tens of thousands of users, the company will face continuous operational pressure and certain pressures as other trading platforms emerge and continue to expand. Market competition risk. Under no circumstances can the project party eliminate, prevent, limit or reduce this competitive effort to compete with or replace the KOK token.

12.4 Risk of uninsured losses

Unlike bank accounts or other financial institution accounts, there is usually no insurance coverage on the KOK token account or the relevant blockchain network. In any case, there will be no public organization to cover your losses.

12.5 Risk of loss of private key

The replacement agent's digital asset KOK token, after extracting its own digital wallet address, the only way to manipulate the content contained in the address is the permutator-related key (ie, the private key or the wallet password). The user is personally responsible for protecting the relevant key and signing the transaction that proves ownership of the asset. The user understands and accepts that this may be irreversible if the private key necessary to access the KOK token is lost or corrupted. The KOK token can only be manipulated by the local or online KOK token wallet to occupy the relevant unique public and private keys. Each replacement should properly keep the private key of its KOK token wallet. If the private key of the KOK token replacer is lost, lost, compromised, corrupted, or compromised, the project party or any other person cannot assist the replacement to access or retrieve the relevant KOK token. In addition, the security of the KOK token wallet (especially the private key) can be preserved in order to enjoy the rewards and gifts attached to the replacement KOK token. KOK tokens should be extracted into the wallet that is absolutely controlled by the user. Once the KOK token has been transferred or transferred for any reason, the unpaid rewards and gifts attached to the KOK token will not be available. The best way to securely log in credentials is for the replacement to separate the keys into one or several places for secure storage, and preferably not to be stored on a public computer. Anyone who obtains the replacement's registered mailbox or registered account access rights by decrypting or cracking the KOK token replacement's password will be able to maliciously claim the KOK token replaced in this public replacement. Accordingly, the KOK token replaced by the replacement in this public replacement may be sent incorrectly to anyone who claims the KOK token through the replacement registration mailbox or the registered account, and the transmission is irrevocable and irreversible. . Each replacement shall take the following measures to properly maintain the security of its registered email address or registered account: (i) use a high security password; (ii) do not open or reply to any fraudulent email; and (iii) strictly keep confidentiality of its confidentiality Or personal information.

12.6 Risk of platform migration or consolidation

The KOK token will initially have a separate underlying blockchain as its own ledger. The KOK token may then migrate to one or more other distributed platforms in the future as long as the platforms are more efficient, valuable, or suitable for transactions executed on the KOK token. In the event of such a migration, all KOK tokens that exist at that time will be converted into new built-in crypto tokens on the migrated KOK token with similar or equivalent technical specifications and functionality. The original blockchain used by the KOK token before migration will gradually die out. Technically, in certain situations, KOK tokens may be merged with other blockchain items to

achieve synergy or based on other valuable considerations. This form of merging may result in the KOK token blockchain being discarded or discarded in exchange for a certain number of cryptographic tokens on the newly created other blockchain. These new crypto tokens will be distributed at a certain exchange rate and distributed to the pre-merger KOK token holder. The compensation that the KOK token holder may obtain in these mergers under a particular valuation model to satisfy 100% of the holder's wishes.

12.7 system upgrade risk

The source code for KOK tokens is open source and may be upgraded, modified, modified or changed from time to time by any member of the KOK Token community. No one can anticipate or guarantee an accurate result of an upgrade, revision, modification, or change. Therefore, any upgrades, fixes, modifications, or changes may result in unpredictable or unexpected results that could significantly adversely affect the value of the KOK token or the value of the KOK token.

12.8 Application lack of attention risk

The value of KOK tokens is highly dependent on the popularity of the KOK token platform. KOK tokens are not expected to be popular, prevalent or commonly used in a very short time after release. Such a lack of interest may have a negative impact on the KOK token application. In the worst case, KOK tokens may even be marginalized for a long time, attracting only a small number of users. In contrast, a large KOK token requirement may be speculative. Lack of users may lead to increased price fluctuations in the KOK token market and thus affect the long-term development of KOK tokens. In the event of such price fluctuations, the project party will not (and is not responsible for) stabilizing or affecting the market price of the KOK token.

12.9 Incomplete information disclosure

KOK tokens are still in development, and their philosophy, consensus mechanisms, algorithms, code, and other technical details and parameters may be constantly and constantly updated and changed. Although the white paper for KOK Token contains the latest key information for KOK tokens, it is not completely complete and will still be adjusted and updated from time to time by the project side for specific purposes. The project party is incapable and has no obligation to inform the participants of every detail of the KOK token development (including its progress and expected milestones, whether delayed or not), so it does not necessarily allow participants to be informed of KOK token development in a timely and sufficient manner. Information generated from time to time. Insufficient disclosure of information is inevitable and sensible.

12.10 Unforeseen other risks

A cryptographic-based token is a new and untested technology. In addition to the risks mentioned in this white paper, there are some risks that the founding team has not mentioned or expected. In addition, other Risks may also occur suddenly or in combination with a variety of risks already mentioned.