云尊币 白皮书

WINCOIN

WINCOIN White Paper

Catalog

1. Foreword

The advent of the Internet has created many wonders and wealth. Almost all the internet trade need to use the qualified third-party credit institutions to handle the payment purpose. These systems are still subject to “ Models that are based on credit.”. The digital assets derived from the blockchain are subverting the third-party credit institutions and facilitating direct payment without the involvement of third parties.

Blockchain is a distributed ledger, it is a technical scheme to maintain a reliable database collectively by using a decentralize and distrust way.

Blockchain is the result of the integration of a variety of technical other than a single technical. These techniques are combined in new structures to form a new way of recording, storing and expressing data.

Anyone can participate in the blockchain network, each equipment can be used as a code and each node is allowed to obtain a complete copy of the database. The failure or attack of each node does not affect the continuous operation of the entire blockchain environment.

Many nodes make up an end-to-end network which does not include centralizing equipment or management mechanism. The nodes are verified by digital signatures without mutual trust. Then the node will propagate and record the data in the nodes of the entire network, the data will never lost and can be traced back, and deception cannot exists between nodes. All the nodes anonymous for mutual trust is not needed between them and they don’t need to public their identity.

The purpose of the application of block chain is to construct a trusted distributed business ecological environment that can realize both self-circulation and expand outwards. It can help millions of physical retailers to open online traffic and offline experiences, and a innovative blockchain business system that combines new retail, new payment, new media together. The subordinate of Winner Dynasty Group, Tiandi Jinghua Chain Store has applied blockchain technology since the initial stage after it was founded. Advanced Pos systems have been installed in each physical store, and the system of more than 200 physical stores provides the fastest and accurate detailed data recently, which enables the managers and operators to speed up the judgment and decision-making on the market by the sharing of data. Physical stores are like the codes of blockchain that can provide the latest information of various markets at any time, and complete the cyclical development of the ecology system of the enterprise of Winner Dynasty Group.

2. Development direction of blockchain

Seen from the development history of the blockchain. The birth of BitCoin makes the technology of blockchain been proved intuitively and truly. However, BitCoin only solves the problem of electronic cash, blockchain can also solve many problems that are closely related to real life expect electronic information problem.

Some people say that BitCoin has no value, but the truth is that BitCoin is like gold at the moment: it has a fixed quantity on the earth and its value is based on market demand.Everyone know how it works, it's like a reserve currency or commodity, nobody has the authority to issue more BitCoin, because the rules of the network are known and cannot be changed. In the future,

institutions will be required to issue these assets in accordance with the contract.

The flow mode of digital assets is flowing point - to - point between the two sides of the transaction, the transactions are settled quickly and they are signed in encrypted form. There is a clear ledger to record or control the chain to maintain the transaction transparent. As a result, the cost and the risk will be reduced, and the fraud will be prevented.

Financial network is a kind of technology platform where people can set up company and operate business. While traditional bank and credit networks are closed platform. If you want to set up a e-commerce network, a payment network like Ailpay or Paypal, or other cash transaction services, you must persuade the current financial institutions to cooperate with you. However, it is difficult to obtain such cooperation, the financial institutions will design a variety of hegemon clause to constraint your normal business practices, which blocks the universal values of fair and free trade. And the birth of BitCoin upended this traditional view of finance.

New product New wealth

Blockchain digital assets

Traceability, vesting, tradable

Be the first bath people who obtains profits from digital assets wealth.

3. What is Wincoin?

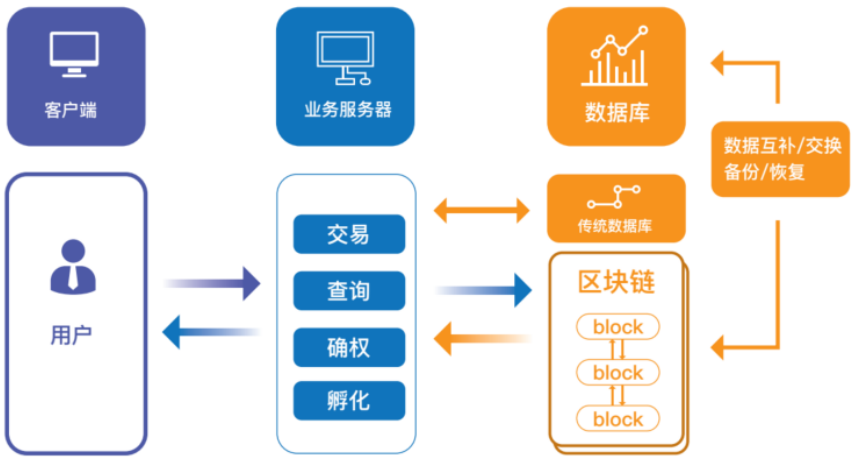
Wincoin is a new type of public chain of DAPPS that is improved on the basis of BitCoin. It

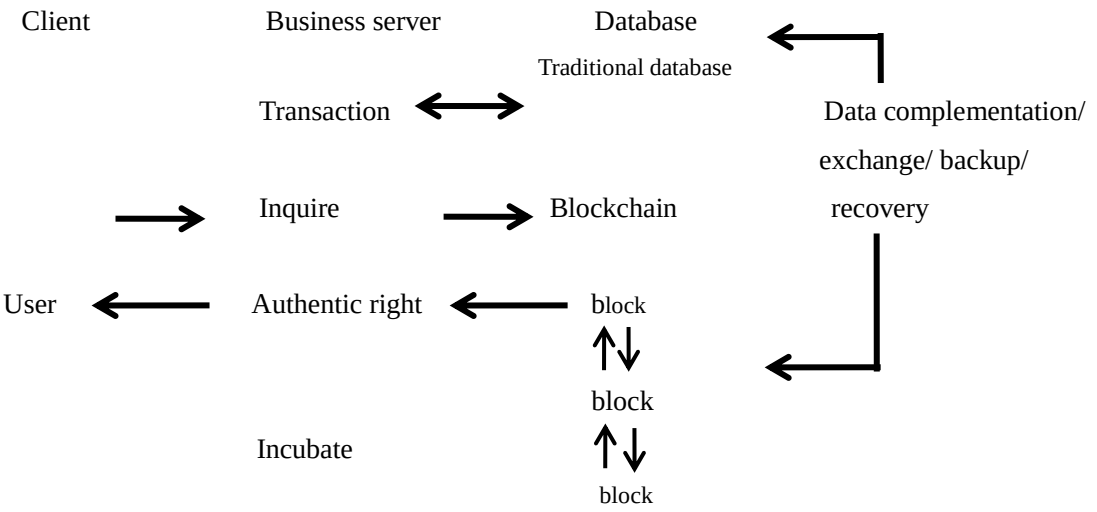
promote the cross-industry coordinated operation of distributed ledger, completes the promotion of offline data and the offline authentication of online data through supporting the trusted authentication gateway of P2P protocol. It is committed to creating a new enterprise ecosystem of online and offline connectivity, which enables ordinary group to access and use blockchain technology and enjoy the enjoy the convenience of it.

4. Technical architecture of Wincoin

We think if the application based on blockchain want to become reliable, the traditional technology system shall be integrated on the basis of the blockchain system, and the blockchain technology shall be properly integrated into the platform. The security of block chain technology and the tamper-resistant characteristics guarantee the reliability of decentralization and the orderly combination of mature technologies guarantee the stable and smooth of the system.

The electronic transactions in traditional banking systems are usually reversible, if someone steals your credit card, you can raise doubts about this transaction. In most cases, the losses are borne by banks or merchants, and consumers do not have to born the losses. This is very convenient for consumers, but financial system is required to be a fairly rigorous integrity network. The allowance of the join of a new member means the increasing of other members' risk. Therefore, it is understandable that the current financial institutions are reluctant to dock with unknown e-commerce sites or e-commerce sites without a strong capital. The Wincoin is different, because the transaction is password-certified and not reversible, so there is no need to restrict access to the network. There is no risk in accepting payments from the people you don't know, this means that the threshold for a merchant or financial intermediary based on the Wincoin will be lowered, which enables honest practitioners to participate in business activities more easily, and all kinds behavior that implied fraud motive will not be implemented. Accepting Wincoin also allows merchants to avoid a lot of administrative overhead and enables the transactions to gain more guarantee.

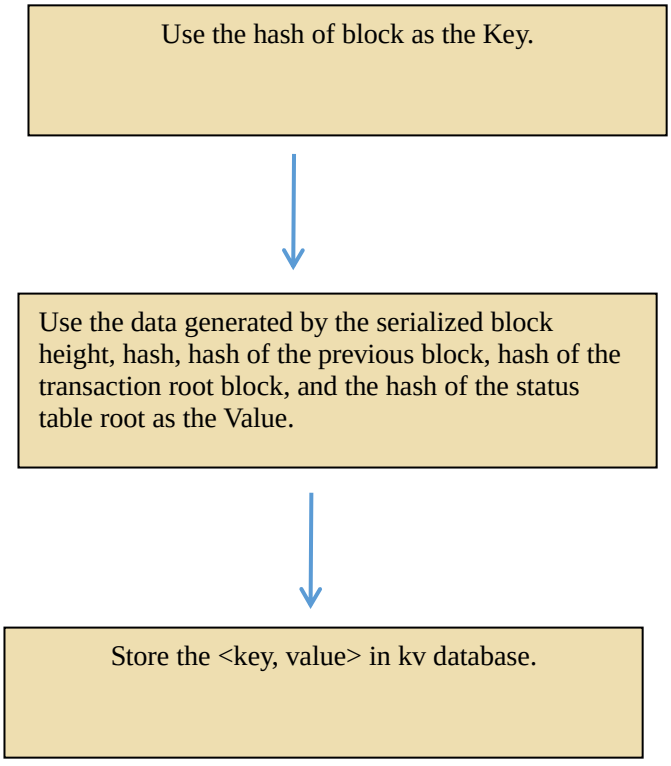


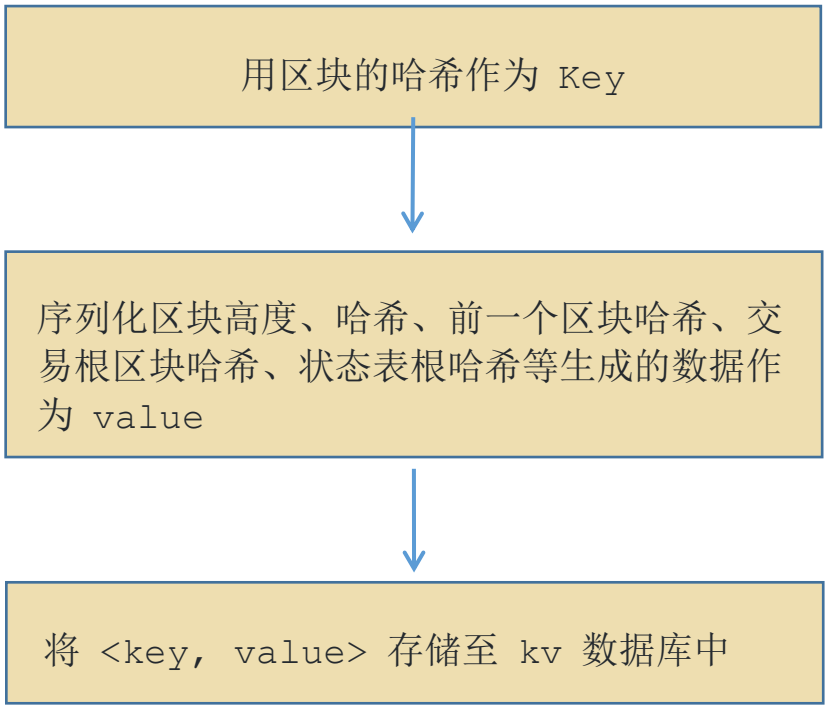


4.1 Data layer of Wincoin

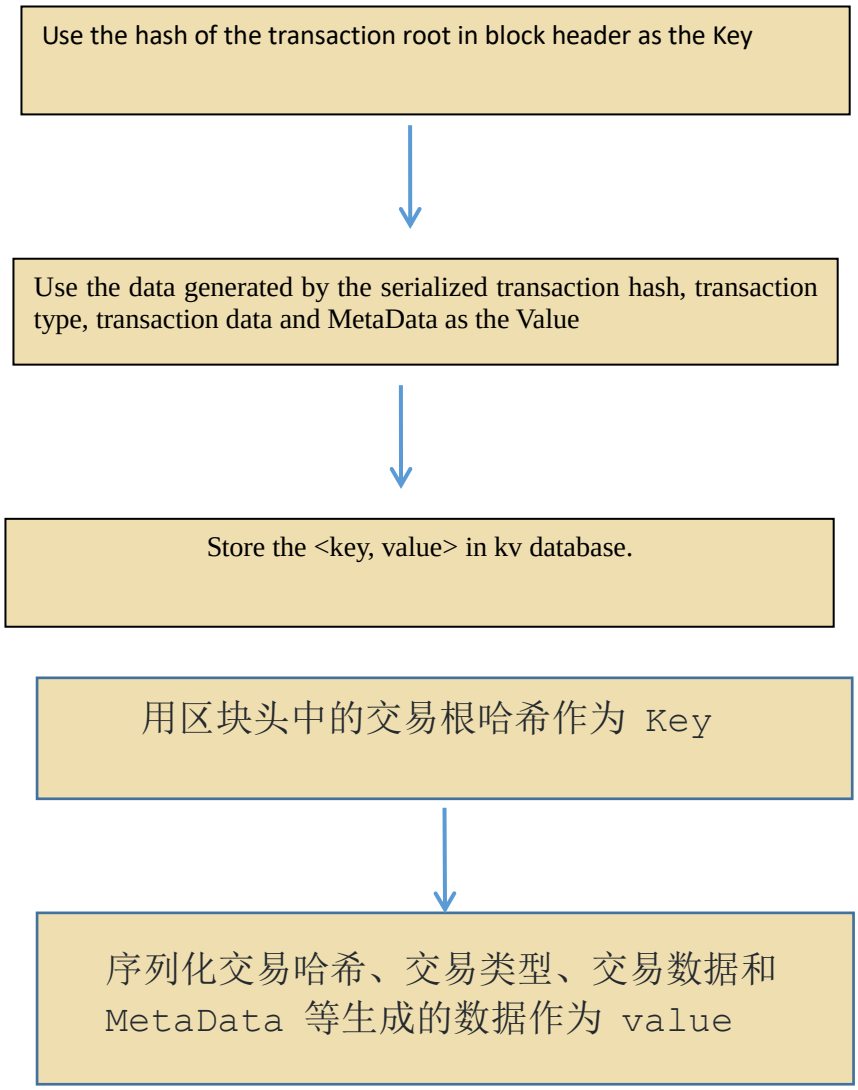
The blockchain data storage system of Wincoin is made up of relationship database and kv database, among which relationship database is used to store information of the block header and specific information for each transaction, while kv database is mainly used to store the data after the serialization of block header, transaction and the status.The main purpose of this process is that you can look for it directly from the relationship database when you simply want to query block header information and specific transactions. And when you want to construct the entire block data, you need to construct block header information from the relational database and obtain the information of specific transaction and status table from kv database according to the hash of transaction root and hash of status table root in block header.

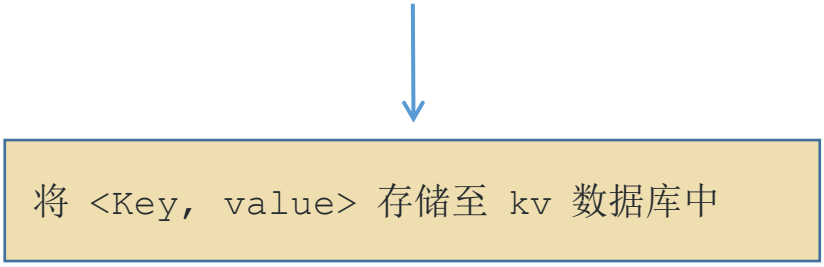
Specific steps of the serialization of the block header information:





Specific steps of the serialization of the transaction：





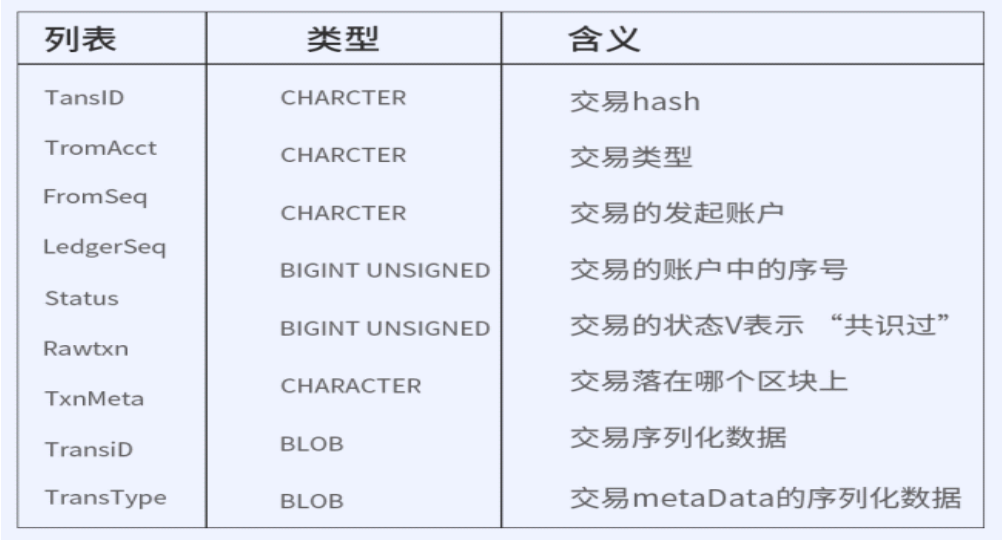
The following tables are the structure of Ledgers and the Transactions table respectively:

List	Type	Implication
LedgerHash	CHARCTER	Hash value
LedgerSeq	BIGINT UNSIGNED	Serial No. of ledger
PrevHash	CHARCTER	Hash value of the previous Ledger
TotalCoins	BIGINT UNSIGNED	The total number of XPP on the current network (transaction may damage the XPP)
ClosingTime	BIGINT UNSIGNED	Closing time
PrevClosingTime	BIGINT UNSIGNED	Closing time of the previous block
CloseFlags	BIGINT UNSIGNED	Solution at the closing time of Ledger(2-1205）
AccountHash	BIGINT UNSIGNED	Closing way of the marked Ledger,it is generally 0.
CloseTimeRes	CHARCTER	stateMap hash of the point of foundation
TransSetHsh	CHARCTER	txMap hash of the point of foundation

列表	类型	含义
LedgerHash	CHARCTER	哈希值
LedgerSeq	BIGINT UNSIGNED	Ledger序号
PrevHash	CHARACTER	前个Ledger的Hash值
TotalCoins	BIGINT UNSIGNED	当前网络上的XP P总数（交易会销毁XRP）
ClosingTime	BIGINT UNSIGNED	关闭时间
PrevClosingTime	BIGINT UNSIGNED	期一个区块的关闭时间
CloseFlags	BIGINT UNSIGNED	iedger 关闭时间的解决放方案（2-120S）
AccountHash	BIGINT UNSIGNED	标识ledger的关闭方式，一般都是0
CloseTimeRes	CHARATER	stateMap 根据点 hash
TransSetHash	CHARATER	txMap根节点哈希

（表：Ledgers）

List	Type	Implication
TansID	CHARCTER	Transaction hash
TromAcct	CHARCTER	Transaction type
FromSeq	CHARCTER	The account that start transaction
LedgerSeq	BIGINT UNSIGNED	Serial No. In the account of transaction
Status	BIGINT UNSIGNED	Status of transaction, V means
Rawtxn		"have been recognized jointly"
TxnMeta	CHARCTER	Which block is the transaction in
TransId	BLOB	Serialized data of transaction
TransType	BLOB	Serialized data of transaction metaData



列表	类型	含义
TansID	CHARCTER	交易hash
TromAcct	CHARCTER	交易类型
FromSeq	CHARCTER	交易的发起账户
LedgerSeq	BIGINT UNSIGNED	交易的账户中的序号
Status	BIGINT UNSIGNED	交易的状态V表示 “共识过”
Rawtxn	CHARACTER	交易落在哪个区块上
TxnMeta	BLOB	交易序列化数据
TransiD	BLOB	交易metaData的序列化数据
TransType		

4.1.1. Characteristics of relationship database (sqlite)

Relationship database was (sqlite) was born in May 2000. As a self-contained and file-based database, SQlite provides excellent tool set that can handle all types of data, has fewer constraints and is easier to use than a relational database hosted on a server.

This is a lightweight embedded database that takes up very low resources, in embedded equipment, it might only need a few hundred K of memory. Its processing speed is faster than the two famous databases, Mysql and PostgreSQL. Sqlite also has the following characteristics:

•Zero configuration, it needn't to be installed and configured.

The core engine of sqlite does not rely on third-party software, when you use it, you needn't "install" it, therefore, you can be free from troubles when you deploy.

•It is a complete database that store in a single disk file.

All the information in the database (such as tables, views, triggers, etc) is contained in a single file. And this file can also be used when it is copied to other directories or other machines.

•Database files can be freely shared between machines in different byte order.

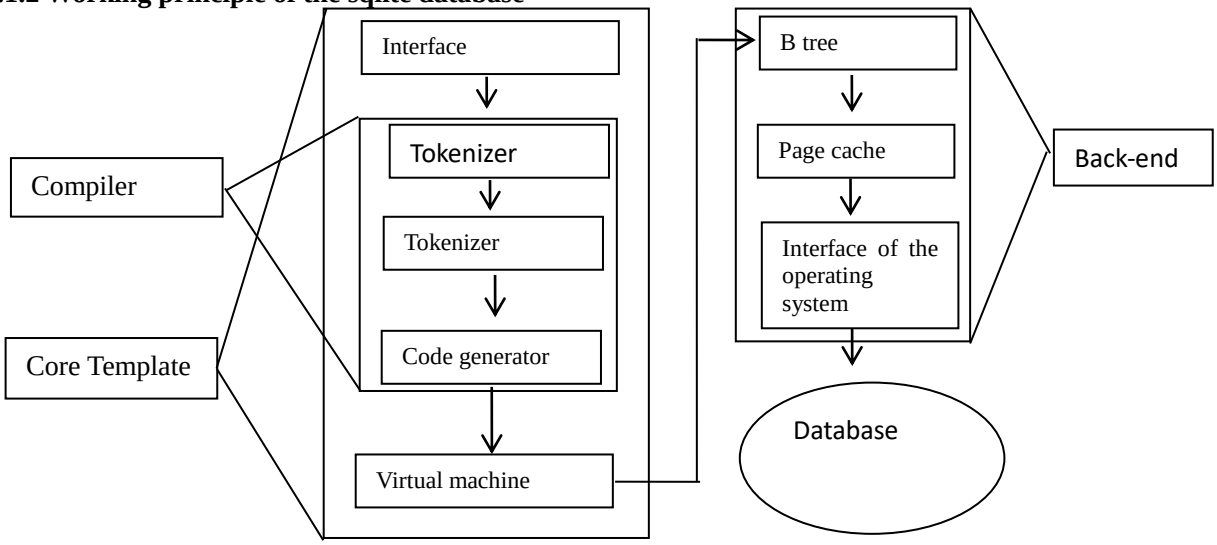
Sqlite supports a variety of systems, it not only supports mainstream operating system but also supports many operating system that are unknown. For example, it supports many embedded systems (such as Android, Windows Mobile, Symbin, Palm, VxWorks, etc.). The database files

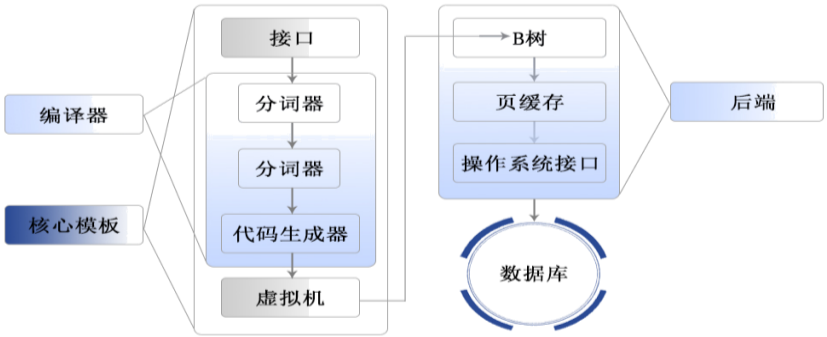
generated by SQLite can be ported in various smart devices, which provides the basis for the popularization of Wincoin to other smart devices.

•It is small enough, the entire source code is about a few hundred KB, therefore, it is capable of running in portable smart devices.

•The operating of data is faster than most databases that are popular at present.

4.1.2 Working principle of the sqlite database





Qlite is mainly composed of component subsystems (that is module), these modules are split into front-end parsing and back-end engines.

Front-end:

The preprocessing of front-end shall uses the SQL statement and the SQLite command passed by the application program. Analyze and optimize the acquired coding, and covert the codes into the SQLite internal byte code that the back-end can execute. The front-end can be divided into three modules:

• Labeling analysis (Tokenzier): divide the input SQL statements into identifiers.

•Grammatical analysis (Parser): the parser analyzes the structure of the identity analysis statement generated by the identifier and obtains a grammatical tree. The parser also contains a optimizer that can reconstitution the grammatical tree, therefore, a grammatical tree that produces an efficient byte encoding program can be found

•Code generator: the code generator traverses the syntax tree and generates an equivalent byte encoding program, and the front-code realized the sqlite3_prepare API function.

Back-end:

The back-end is the engine that explains the byte encoding program, and the engine does the real database processing work. The back-end is composed of four modules.

•Virtual machine (VM): VM module is an interpreter for the internal byte encoding language. It realize the work of SQL statement through executing byte encoding statement. It is the ultimate operator of data in a database. It regards the database as a collection of tables and indexes, while tables and indexes are a series of tuples or records.

•B/B+ tree: B/B+ tree module organizes each tuple into a tree data structure that has been sorted in one-time., tables and indexes are placed in separate B+ and B trees. This module helps the VM to search, insert and delete tuples in the tree. It also helps the VM to create new tree and delete old tree.

•Page scheduler（pager): the page scheduler module implements a page - oriented database file abstraction at the top of the original file. It manages the in-memory cache (database page) used by B/B+ tree, in addition, it also manage the locking of other files, and use logs to implement the ACID properties of things.

•Operating system interface (system interface): the operating system interface module provides a uniform interface for different local operating systems. The back-end realizes the sqlite3_bind_*,sqlite3_setp,sqlite3_coloumn_*,sqlite3_reset and sqlite3_finalize API function.

The characteristics of the relational database can meet the requirements of the operation of cloud Wincoin in portable smart devices, and can be transplanted in the operating system of various technical architectures without big change, which guarantees the rapid promotion and popularization of Wincoin in general group.

4.2 Encryption algorithm

The basic process of data encryption is to process the file or data that is originally proclaimed in writing into a piece of code that is unreadable by using a kind of algorithm. Currently, the encryption algorithms that are commonly used in blockchain are symmetric encryption, asymmetric encryption, public private key, Hash algorithm and so on.

Symmetric encryption: symmetric encryption is the fastest and simplest type of encryption, the same secret key is used for encryption and decryption. Symmetric encryption usually uses a relatively small secret key, which is usually less than 256bit. The seize of the secret key should be both safe and efficient, and it is a trade-off.

Asymmetric encryption: asymmetric encryption provides a very secure way for the encrypt ion and decryption of data, it uses a pair of secret keys, public key and private key. The private key can only be safeguarded by one party and cannot be leaked, while the public key can be issued to anyone who requests it. Asymmetric encryption uses one of the secret keys to encrypt, while decryption requires another key.

Private key: non-public, it is a 256 bit random number that is kept by the user and is not open to the public.The private key is usually generated randomly by the system, which is the only proof

of the right t use users' account and the ownership of the assets in the account. The effective bit of it is so long that it can't be breached and there is no safety hazard.

Public key: it can be disclosed, every secret key has a public key that matches it. The Ecc public key can be generated by the private key through a one-way, deterministic algorithm, the schemes that are commonly used include: secp256r1 (international standard), secp256k1 (BitCoin standard) and SM2 (Chinese national standard), Photon chain and initial data chain select secp256r1 as the secret key scheme.

Hash algorithm: usually hash algorithm means SHA (Secure Hash Algorithm), this algorithm is designed by the NSA and the series of cryptographic hash functions issued by the NIST include variations of sha-1, sha-224, sha-256, sha-384, and sha-512. At present, BitCoin adopts SHA-256 algorithm. Hash algorithms in Photon chain all refer to SHA-256 expect PW.

Wincoin has improved on this basis, the homomorphic encryption used in it is a method that execute calculation without decrypting the encrypted data in advance. It provides an urgently needed method which use blockchain technology on the original basis. The data stored data on the blockchain can achieve a perfect balance by using homologous encryption technology, and it will not cause any significant change to the blockchain property. In other words, the blockchain is still a public blockchain. However, the data on the blockchain will be encrypted so that the privacy issues of the public blockchain dealt. Homomorphic encryption technology enables the private block chain to have the privacy effect of private blockchain.

4. 2. 1 Processing process of homomorphic encryption algorithm

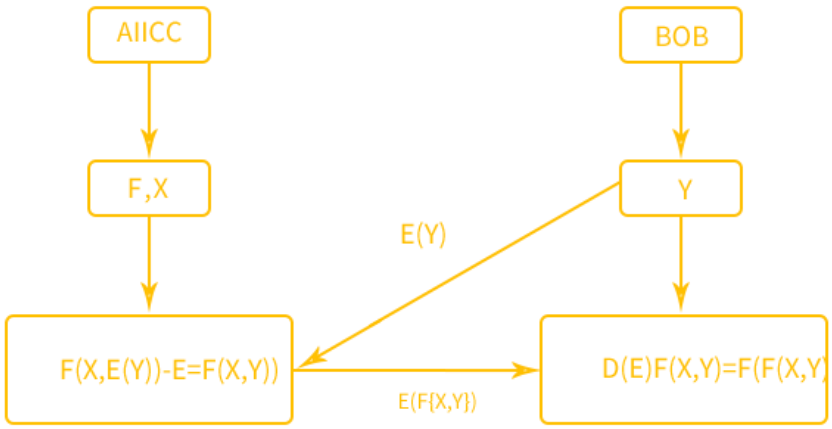


图3 加密信息处理

Figure 3 Processing of encrypted information

As shown in figure 3, it is mainly to protect the private information. Alice has private function fA and private information XA, encrypted private information yB with private public key pkB to get E(y) and send it to Alice, Alice use its own private function fA to encrypt private information XA and E(yB). Because of the homomorphism, the function fA is hidden, and Bob gets E(fA (XA, yB)). Bob encrypts D(fA (XA, yB)) =fA (XA, yB) by private key.

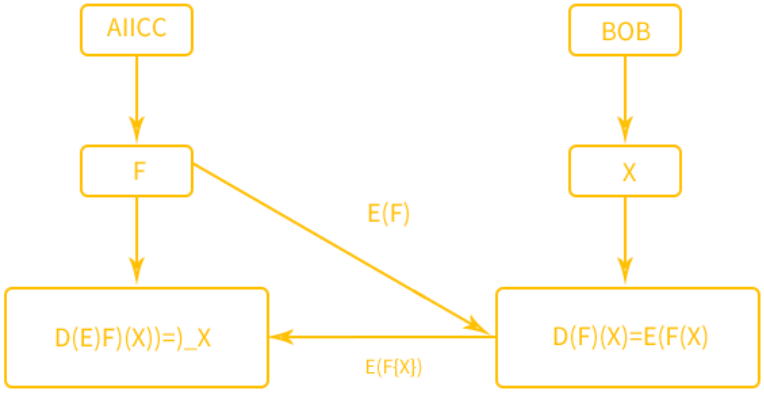


图4 加密函数处理

Figure 4 Processing of encrypted function

As shown in figure 4, it is mainly to protect the private operation function. Alice has a private function fA, which is sent to Bob after been encrypted by the private public key pkA, and Bob calculates E(fA)(XB) based on private information. Because of the homomorphism, Bob's information XB is hidden, and E(fa(XB)) is obtained and sent to Alice, Alice decrypts it with private key and get fA(XB).

Homomorphic encryption technology not only provides privacy protection, but also allows access to encrypted data on the common blockchain for auditing or other purposes. In other words, use homomorphic method to encrypt the data stored on a common blockchain can provide the best part of the public blockchain and private blockchain.

If E is a fully homomorphic function for function_a, that is

There is a constructible function operation function_b, which makes it

In which, the encryption operation is E, plaintext is m, and e is get after encryption. If you can construct the corresponding function_b for E when you operate function_a on any complex plaintext, then, E is a homomorphic encryption algorithm for function_a. The purpose of purpose of all homomorphic encryption is to find an encryption algorithm that can perform any number of addition and multiplication operations on the encrypted data, which makes the result obtains after a certain operation on the encrypted data exactly equals to the ciphertext obtained from the encryption after the perform expected operations on on the data that has not been encrypted.

4.3.Use Netty to to build high-performance and highly available decentralized networks

4.3.1 I/O module of Netty

Based on the realization of non-blocking I/O , the underlying dependencies are the Selector for the JDK NIO framework.

Selector provides the ability to select a task that is ready. Briefly, the Selector will constantly poll the Channel that is registered on it, and if a Channel has a new TCP connection to access, read, and write events, the Channel is in a ready state and it will be polled out by Selector. Then a set of ready Channels can be obtained through SelectionKey and perform subsequent I/O operations.

A multiplexer Selector can poll multiple channels simultaneously, since the JDK1.5_update10 version (+) is realized by using poll to instead the traditional select, it does not have the limit of the maximum connection handle 1024/2048. This means that thousands of clients can be accessed with only one thread to take charge of the poll to Selector, which is exactly a huge technological advance.

After using the non-blocking I/O module, Netty solves the performance, handling capacity, and reliability problems brought by the traditional synchronous blocking I/O.

4.3.2. Thread scheduling module

There are three commonly used Reactor threading models respectively as follows:

Reactor single-threaded model: Reactor single-threaded model means that all the I/O operations are performed on the same NIO thread. For small volume application scenario, the single-thread model can be used.

Reactor multithreading model: The biggest difference between the Rector multithreading model and the single-threaded model is that there is a set of NIO threads that handle I/O operations. It is mainly used in high concurrency and big business volume scenarios.

Principal and subordinate Reactor multithreading model: the characteristic of the principal and subordinate Reactor multithreading model is that it is no longer a single NIO thread for receiving client connections in server, it is a separate NIO thread pool. The principal and subordinate Reactor multithreading model can be used to solve the problem that the listener thread of one server cannot effectively handle the poor performance in all client connections.

In fact, the thread model of Netty is not fixed and, the three above mentioned Reactor thread model can be supported through creating different EventLoopGroup living example in the starting of auxiliary class and configuring appropriate parameter.

In most scenarios, concurrent multithreading can improve the concurrency performance of the system.However, if the concurrent access to the shared resources is not handled properly, there will be serious lock contention, which ultimately leads to performance degradation. In order to avoid the performance loss brought by the lock contention, serialization design can be adopted (message processing is done within the same thread as much as possible, thread switching is not performed during message processing so that the multithreaded competition and synchronized locks can be avoided.).

In order to improve the performance as much as possible, Netty adopts serial lock-free design, and perform serial operation within the he I/O thread to avoid performance degradation cause by multithreaded competition. Superficially, the CPU utilization of serialization design seems to be low and the concurrency is not enough. However, multiple serialized threads can be started

simultaneously and operated concurrently through adjusting the thread parameters of the NIO thread pool. The performance of this local lock-free serial thread design is better than a queue-multiple worker thread models.

4.3.3 Serialization formats

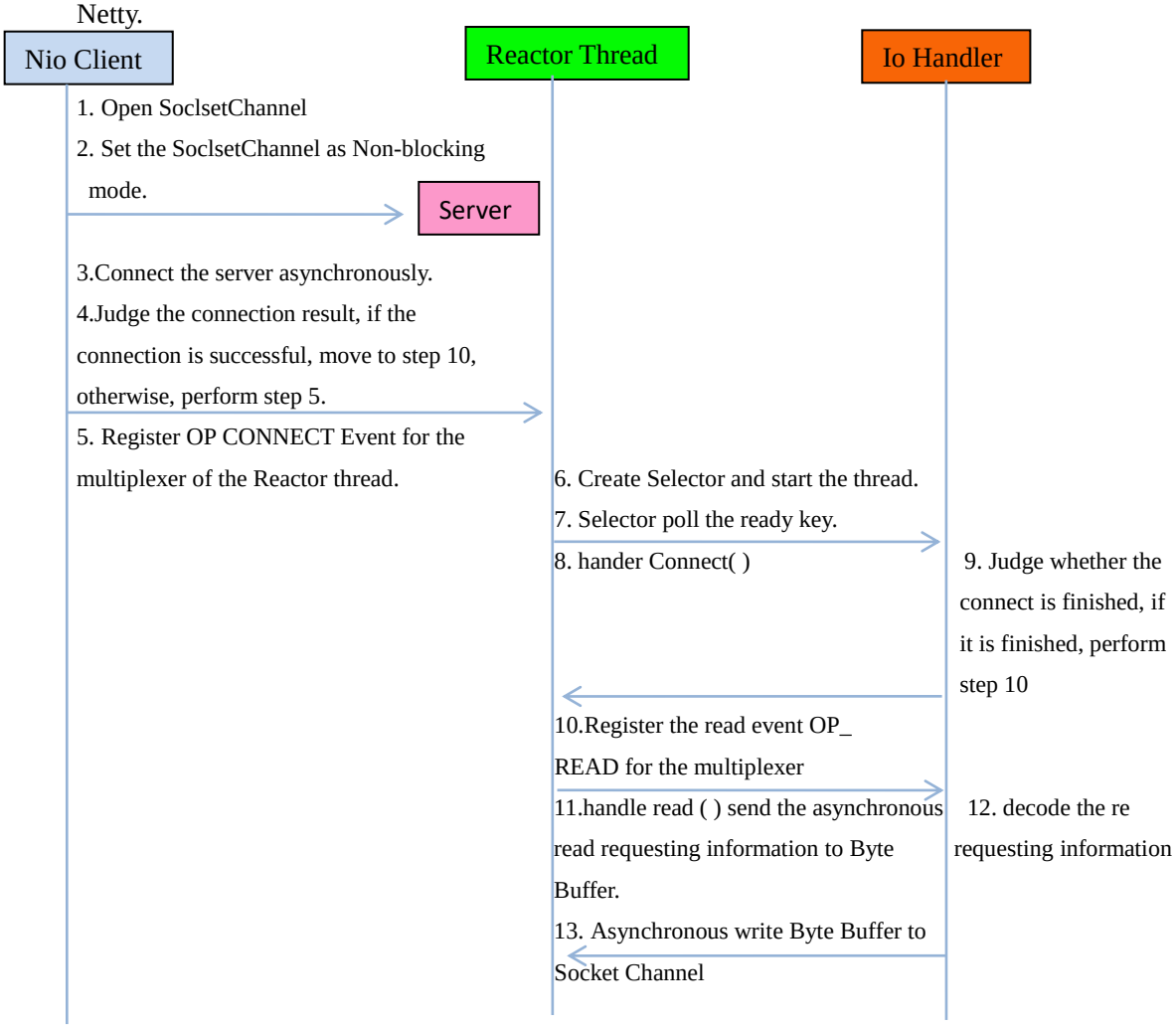
The key factors that affect the serialization performance are summarized as follows:

The size of the bite rate after serialization (occupancy of network bandwidth), serialization & deserialization performance (occupancy of CPU resources).

Performance of concurrent calls: stability, linear growth, and occasional time delay burrs are used to test the performance of Java serialization and binary coding respectively, the code is tested 1 million times, and the test result shows that: the performance of Java serialization is only about 6.17% of binary code.

Netty provides support for GuGe Protobuf by default, users can realize other high-performance serialization frameworks (such as compressed binary encoding and decoding framework of Thrift) by extending Netty's encoding and decoding interface.

Different application scenarios have different demands for the serialization framework, Netty has provided the Protobuf binary serialization framework of Google to high-performance application scenarios. If users have demands for other binary serialization frameworks, it can also be realized on the basis of the extension of the encoding and decoding framework provided by Netty.



4.3.4 The reasons for using Netty framework

1)Design

Uniform API for different protocols (blocking and non-blocking).

Driven model based on flexible, extensible event.

Highly customizable thread model.

Support of reliably connectionless data (UDP).

2) Performance

Better handling capacity and low delay.

Save more resources.

Minimize unnecessary memory copying as much as possible.

3)Security

Full SSL/TLS and STARTTLS support can work well with the restriction environment of Applet and Android.

4）Robust

OutOfMemoryError may not be caused by fast connection, low connection or overloading connection.

The problem that the read frequency and write frequency of NIO is inconsistent will not occur in high speed network environment.

5)Easy to use

Perfect JavaDoc, the user guide and sample are concise and simple.

Just relies on JDK1.5.

The Netty framework can bring better compatibility, security, stability and maneuverability to the Wincoin，and provides a basis for the rapid read and write of the versatility application of the Wincoin.

Big data field: PRC framework of the high-performance communication and serialization component Avro of classical Hadoop uses Netty to perform cross node communication by default. Its Natty Service is realized on the basis of the secondary encapsulation of Netty framework.

Large data computing usually uses multiple compute nodes and one /N summary nodes to carry out distributed deployment, a huge amount of data exchange exists between the nodes. For Netty's overall performance is the highest among the NIO frameworks that are mature, it is usually selected as the communication between the nodes of the big data.

Enterprise software: the integration of enterprise and IT requires ESB, Netty’s support for multiple protocols and the simplicity and high-performance of the customizing of proprietary protocols are the preferred communication module for ESB PRC framework. In fact, bus manufacturers of many enterprise are likely to choose Netty as the basic communication communication module to be used in the IT integration of enterprise.

Communication industry:Netty's advantages of asynchronous high performance, high reliability and high maturity make it widely used in the communication industry.

4.4. Consensus mechanism of Wincoin

Wincoin adopts the hybrid consensus mechanism of PoW+PoS, which can maximize the audience. Users who hold the Wincoin and miners can participate in the voting and participate in major decisions jointly. Digital asset holders and miners can influence pre-programmed updates, this is truly decentration.

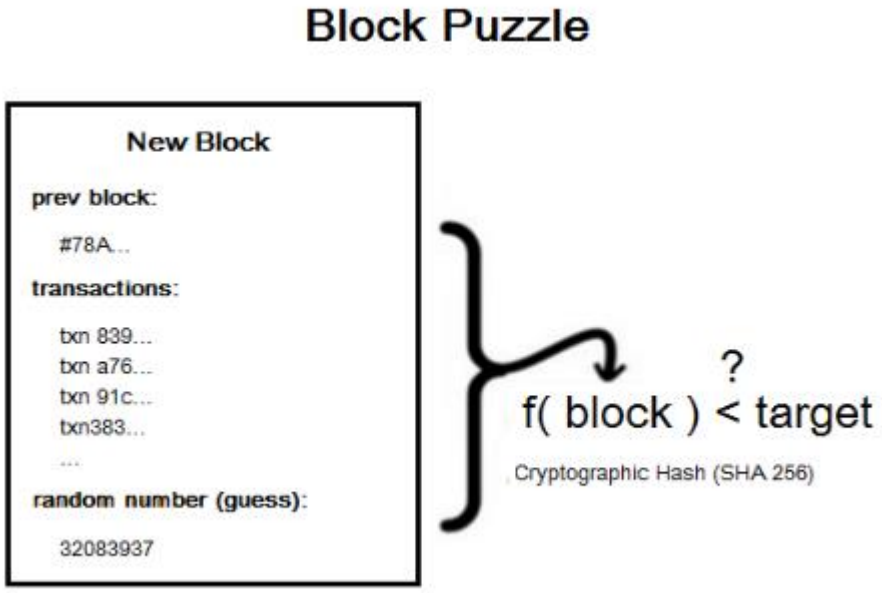
4.4.1 The process the proof of POW work

POW is a widely tested solution that also has anti-attacking performance and extensibility. We can summarize the steps of work proof as follows:

Generate Coinbase transaction and make a list of transactions with all other transactions that are ready to be packaged into the block. Generate Merkle Root Hash by using Merkle Tree algorithm.

Assemble the Merkle Root Hash and other related fields into the Block Header, and 80 byte data of the Block Header is input as proof of work.

Constantly change the value of the random number (nonce) in the Block Header, perform double SHA256 operation on the Block Header after each change (SHA256(SHA256(Block_Header))), and compare the value with the target value of the current network. If the value is less than the target value, the problem is solved successful and the work proof is completed.



4.4.2 Proof of Stake

In the proof of work, each node assists in creating and validating new blocks. The reward and contribution is proportional to the power resource of the entire network. The risk of malicious attacks or malicious deception of other nodes may also occur. The system of the proof of stake tries to keep the benefits of the work proof first and eliminates some potential security issues.

The proof of stake can be used to reinforce the proof of work other than replace it. It can simply be an additional step to add and approve new blocks.

- The rational logic behind PoS.

(1）Enables the owner of the stake to vote to determine the bookkeeper.

(2）Maximize the dividends of the owner of the stake.

(3）Minimize the consumption on the guarantee of network security.

(4）Maximize the performance of network.

(5）Minimize the cost of operating the network.

The benefit of the design of Wincoin is that the owner of the stake has the right of control. The fundamental characteristic of PoS is that the owner of the stake retains the right of control, thereby decentralizing the system. It can improve the security of blockchain digital assets because the the potential risk of a 51% attack may exist in the work proof, the people who hold most of the power resources will be able to control the entire network easily.

On technology level, Wincoin applies the voting mechanism for blocks (a flexible and practical PoS mechanism). In addition, a new hybrid consensus mechanism is obtained by combining the double chain structure and the enhanced PoW mechanism of the pole-mining idea and the PoS mechanism. In this new hybrid consensus mechanism, keyBlock must get enough votes to be considered legitimate, so both PoW and PoS can participate in the consensus consensus and play an important role.

4.5 Use Wincoin to deal the disadvantage that the network speed of the blockchain is slow

How does Wincoin solve the problem that the network speed of the blockchain is slow? It is realized through “RingBuffer” and “Disruptor”. The Disruptor is an open source concurrency framework that enables the realization of the concurrency operation of the network's Queue without a lock. Why is the “Disruptor” so fast?

(1)The disadvantage of the lock

The Disruptor doesn’t use lock at all. Instead, we use CAS (Compare And Swap/ Set) operation at the place where we need to make sure that the operation is thread-safe (in particular update the next available serial number in a multi-producer environment). CAS operations consume less resources than locks, because they do not involve operating systems, and can be operated directly on the CPU. All visitors record the realization way of serial number, multiple producers are allowed to share the same data structure with multiple consumers. The serial number can be traced in each object (ring buffer, claim Strategy, producer and consumer), adding the magic cache line padding means there is no false sharing and unanticipated competition.

(2) Filling of cache line

All operations and procedures are performed by CPU. RAM is the place where your data (including code line) stores. The goal of Disruptor is to be operated in memory as much as possible. If you access a long array, when one of the values in the array is loaded into the cache, several other values will be loaded additionally. Therefore, can transverse this array very quickly. In fact, you can transverse arbitrary data structures that are allocated in contiguous memory blocks.

(3) False sharing

(4) Demystify the memory barrier

As another CPU-level instruction, memory barrier does not cost as much as a lock. The kernel does not intervene and dispatch between multiple threads. But everything comes after costing a lot. Memory barriers do have expenditure—the compiler/CPU cannot reorder the instructions, as a result, the CPU can not be used as efficiently as possible. Meanwhile, the refreshing of cache also has expenditure.

The realization of the Disruptor minimizes the read and write frequency of the serial number. Each read or write of a volatile field is a relatively high cost operation. We should also realize that Disruptor would perform well when it is in batch.

We use the data structure of Disruptor and Ring Buffer because they provide us with reliable messaging features. This ground is good enough, but it has some other advantages. Firstly, Ring Buffer is faster than chain table, because it is an array and has a predictable access pattern.This is great , for CPU-cache-friendly-data can be preloaded at the hardware level to the cache., therefore, CPU does not need to return to RAM frequently to find the next data of Ring Buffer. Secondly, Ring Buffer is an array where you can pre-allocate memory and keep the array element valid forever. Which means that the memory garbage collection (GC) does not need to do anything in this situation. In addition, it is not a like a chain table that when a data is added, the object need to be created, and when these data is deleted from the chain table, these objects needed to be cleared off.

5.Application of Wincoin

5.1 Ecology of the enterprise of Winner Dynasty Group

Ecology of the enterprise of Winner Dynasty Group is a new business model which maximizes the benefits by creating and sharing of the merchants in the system, the development trend and value of it will be increasingly manifest as time pass by. It is based on the development of blockchain technology and its application in business pattern has been supported and approved by millions of participants in dozens of countries. Winner Dynasty Alliance has created a new blockchain enterprise ecosystem through the application of the strong data collection and analysis ability and the cross-boundary integration of block chain technology.

Ecology system of the enterprise of Winner Dynasty Group creatively associates the block chain technology with community construction, social media, business promotion, physical business circle, advertising promotion, e-commerce, etc. Establish an open and transparent personal credit platform through the continuous deposition of the verifiable transaction data. Combine the identity, transaction data and credit system of the user to build a new blockchain ecosystem based in the identity and credit.

5.2 Characteristics of the Wincoin

5.2.1 In commercial applications

(1) Blockchain service

Wincoin provides multilingual block chain data access and interaction interfaces to allow more Wincoin holders or merchants to dock their applications on the platform.

(2) Business logic

Cooperating with traditional architecture, Wincoin deals orders and matchmarking transactions in the business layer. After completion, the transaction is broadcast on the blockchain, the settlement is completed and the users' experience has improved.

(3) Data storage

Uplink storage should be performed on the important data that cannot be tampered, carry out hash calculation on all kinds of information, and store it in the block to ensure that the data security cannot be tampered.

(4) Network protocol

The underlying protocol of the block chain adopts point-to-point networking protocol, and each node participates in the maintenance of network integrity -- data validation and data forwarding, etc. The integration of smart contract through Wincoin has simplified the application

and development of blockchain.

5.2.2 In technological architecture:

(1) Dealing the affairs safely, fast and efficient at the speed of thousand affairs per hour.

(2) Provide an incentive mechanism for all staff to protect the network and expand globally with the smallest resource footprint.

(3) Upgrade the system whose core is having a separate payment function on the basis of providing basic transaction of digital assets.

(4) Use a agile architecture to promote the adding of new core features allowing the creation and deployment of advanced applications.

(5) Operate on a wide range of devices, including mobile devices.

5.3 Member structure of the ecology the enterprise of Winner Dynasty Group

Five roles in the ecology system of the enterprise.

Company HQ, Yunbao Web, Yunbaotong App, Business Alliance, Members of Winner Dynasty

The details are clear at a glance to fully guarantee the financial safety of each role.....

B Yunbao Web
Market promotion
Pre-sale and after-sale service

C Yunbaotong App
Coverage of mobile market
Realize Yunbao service

D Business Alliance
Publish goods and services
Accept the consumption online and offline

E Members of Winner Dynasty
Encrypt digital assets
Enjoy the rebate of integration

Comprehensive control mechanism, the details is clear at a glance.

While satisfying the basic functions, the enterprise alliance management system has a comprehensive control mechanism for the settlement of the amount of the stored-value, the sharing of consumption profits and the management of integration circulation to fully guarantee the financial safety of each role. The details of stored-value, integration and rebate are clear at a glance.

5.4 Application tools for the ecology chain of the enterprise of Winner Dynasty Group

Forgame

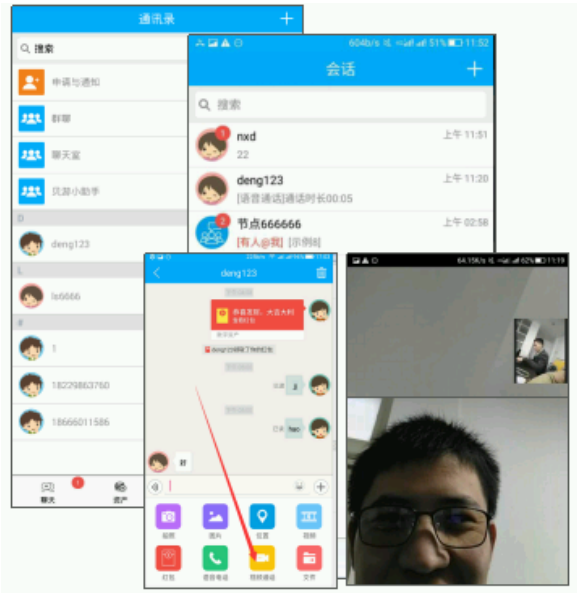
It is a multi-function social tool developed on the basis of blockchain technology, and a platform that integrate the blockchain application of the enterprise alliance of Winner Dynasty Group .

It is a chat application that offers users the option to chat with an unlimited number of users around the world. People can also share their passion or interest to interact through various groups or chat rooms.

It is a digital assets management application that has incorporated a variety of digital currencies and realized multi-management by one application.

It is a merchant platform, many merchants who support digital asset payment has checked in to realize shopping payment function.

It is a promotion platform that can increase the pleasure of chatting and promote the circulation of digital assets through sending out Red Packet.



5.5. Process of the ecosystem of the enterprise of Winner Dynasty Group

5.5.1. Commercial value

The merchants that has join the ecosystem of the enterprise of Winner Dynasty Group can handle the affairs in the business process efficiently, quickly and simply and provide the administrator with diversified services like decision-making basis, marketing promotion, data statistics. And the founders of the enterprise alliance can get more profit and speaking right. Merchants unite to form alliances. Consumers can use the Yunbaotong App of the ecology of the enterprise of Winner Dynasty Group to consume, enjoy discounts, gain the rebates of integration and exchange gifts, etc.

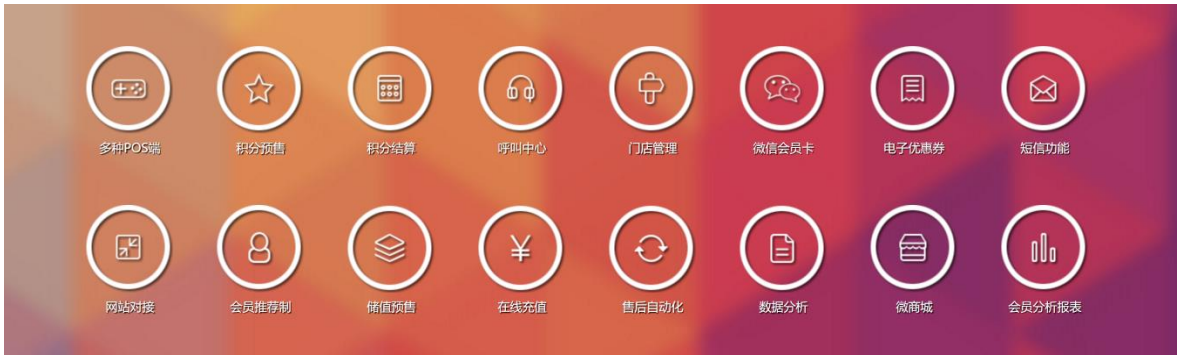
（1）Merchants in the same industry or different industries can use it.

（2）Unified alliance and share customer resources jointly.

（3）Members can enjoy discounts and integration everywhere by using Yunbaotong App.

5.5. Main function module

It is not only a simple management system for enterprise alliance, we can do more things for you.....

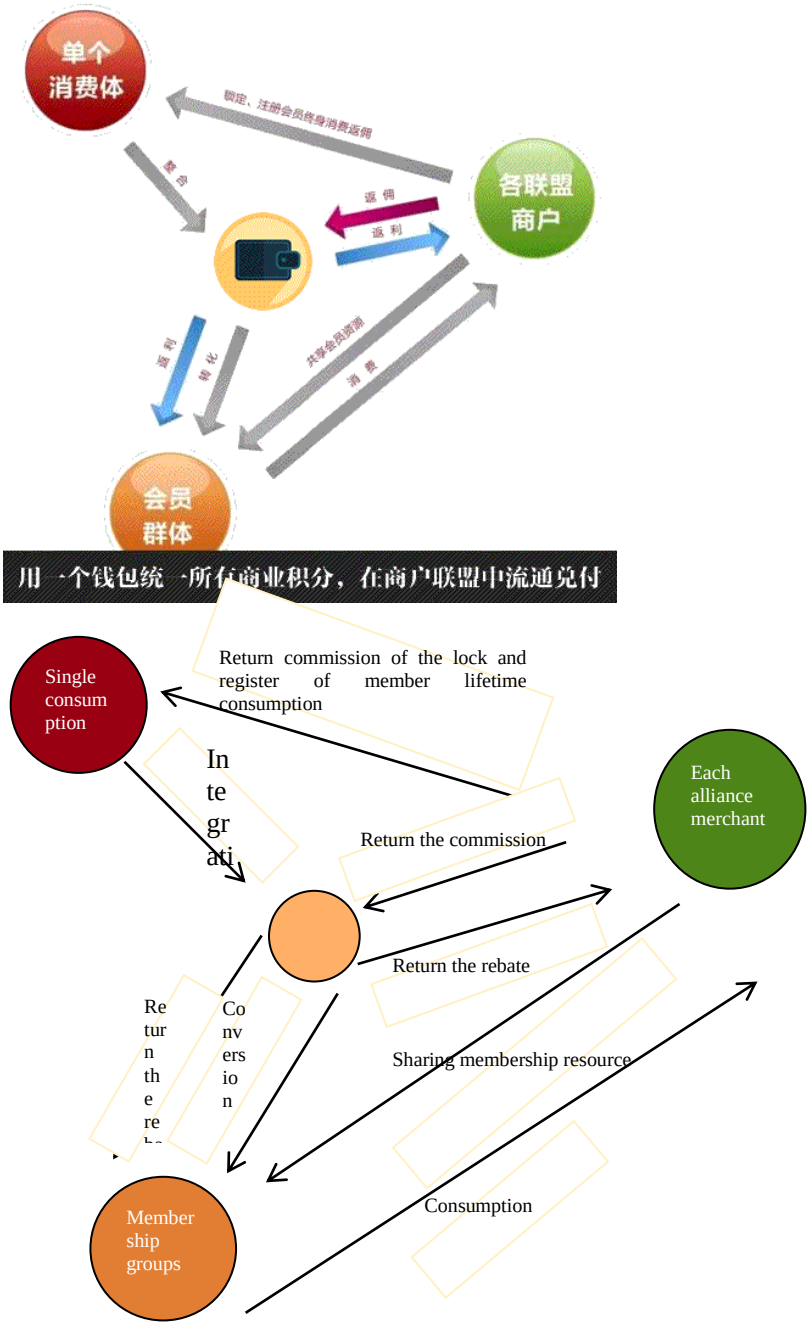


Various Pos end Pre-sale of integration Settlement of integration Call center Store management WeChat membership card Electronic coupon Message function
Website docking Membership recommendation system Pre-sale of stored-value Online top-up Automation of after-sale Data analysis Micro mall Report of member analysis

5.6 Extension of the application of Wincoin

The distributed ledger technology on the blockchain connects the digital asset flow on the blockchain with the real cash payment. From function of the blockchain payment, blockchain payment is similar to Google Wallet and Ailpay Wallet. But because it is set up on the basis of the decentralized P2P credit, it has exceeded the limits of country and region, it can play the role of the efficient and low-cost value transmission that traditional financial institutions cannot replace in the global internet market.

The blockchain credit system from information to value network. Everyone’s password wallet can be developed into a "self-financing" platform, it can the cause the liquidation of the accounts kept in the entire network through P2P payment, deposit, transfer, exchange and debit. It can issue its own financial contract products and credit IOU through Wincoin.



Use a wallet system to realize the payment of all the business integration in merchants alliance in a circulation way.

5.6.1 User exchange domain

The Wincoin system framework is ideal for deployment in portable smart devices,a lightweight Dapp App can be installed on a smart phone with a small amount of storage space in the smart phone, and realize the possible that the smart phone is the code of the whole blockchain system and make the entire network more stable. The profit in the business model comes from the transfer and transaction between the merchant, the individual and the bank, Wincoin provides the service of deploying the efficient blockchain solutions quickly.

Digital money can play a very important role in electronic commerce, retail payments and transfer between individuals and individuals, the value generated from circulation and boundary of the circulation scope determines the value. Users can use the smart phone as a communication node, based on the node reward mechanism, they can get the digital assets awarded by the application. These digital assets can be used to exchange commodity, consumption, etc, which encourage users to use Dapp App. The digital assets can also be used to send red packet, which accelerate the circulation of digital assets and promote the use of Dapp App in groups, and create unique value system.

5.6.2 E-commerce domain

At present, the services provided by e-commerce platforms provide are still centralized services. Well-known e-commerce platforms Alibaba, Amazon and other big e-commerce companies have imposed strict controls on sellers , adopts the business model of competitive bidding, charge fees for the platform, some of the companies even have high commission. Compress the seller's interest to ensure the profit of the platform. The cost of the sells is high all the time, which may may lead to a loss in the end.

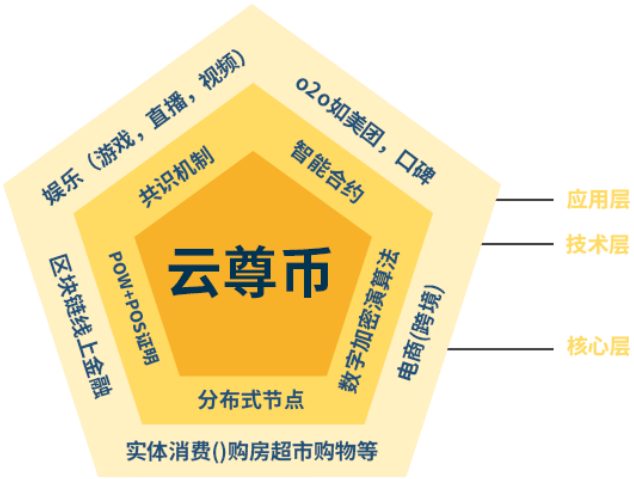
The greatness of the Internet business model is that it has created the professionalism of the digital currency trading system, reduced the intermediate links, and reduced the opaque black box operation in business activities. It has realized the decentralization that makes the whole transaction transparent. Therefore, it is not surprising that digital money becomes a standard configuration of global e-commerce.

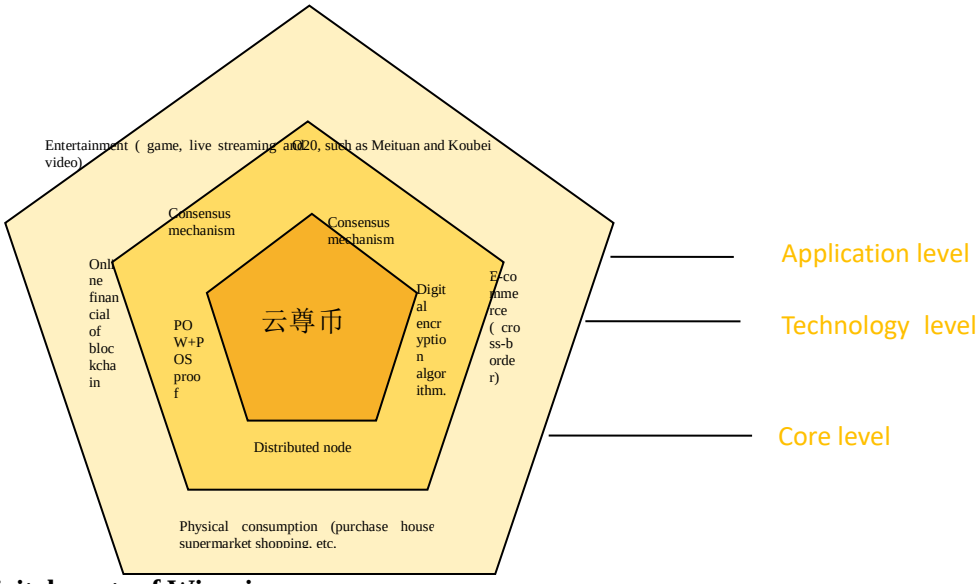
The enterprise alliance of Winner Dynasty links the buyers and sellers together directly on the basis of the application of the e-commerce Dapp App of Wincoin, and centralized third parties aren't needed to link the parties. So there is no transaction fee, and the decision of personal data is held by the users. The realization of the vision and goals of "free transaction" will generate great impact on the current e-commerce models.

E-commerce platform

5.7 Development plan of Wincoin

Wincoin is a new type of public chain of distributed ecological application (DAPPS) improved on the basis of BitCoin. As a industrial application ecological open source project, it expand the block chain technology application scenario, provide economic and social ground application in various fields (such as the application in Financial sector (payment, transaction clearing, trade finance, digital currency, equity, private equity, bond, financial derivatives, crowd-funding, credit, risk control, credit investigation) and has been extended in other industries (020, medical health, IP authorization, Internet of things, education, social management, etc.) on the basis of pegged sidechians technology and create a commercial ecological complex based on block chain technology. It provides diversified services for any country, industry, and any field in the world and uses distributed ledger to reshape the current Internet service model and create infrastructures for the next generation value internet and build blockchain ecology.





6. Digital assets of Wincoin

6.1 **Issuance of the digital assets**

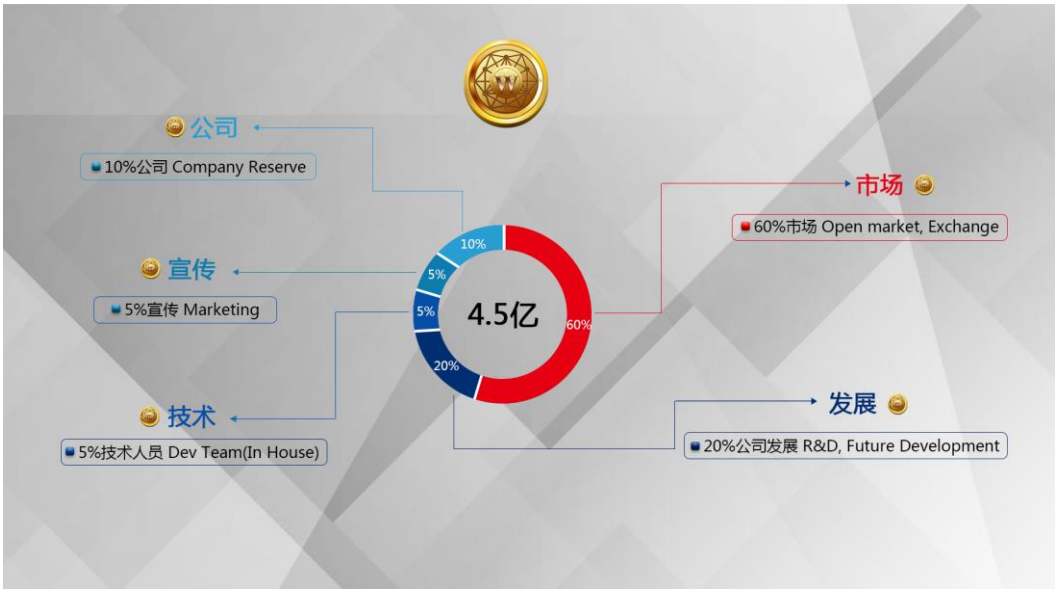
As a blockchain platform, Wincoin runs a system digital assets in the system to maintains the the normal operation of the whole system economic system. Wincoin, whose English abbreviation is WC, is the symbol of the value system of Winner Dynasty Alliance.

It is created for the general public and fully and effectively uses the block chain technology to ensure its security. Recognized by several countries makes it easy to convert into local currency and it is accepted by many alliance merchants. Wincoin is expected to add more new features, which make it more dynamic and attract a larger user group, and e-commerce will be used as its main driver.

Version: Wincoin 3.0
Chinese name: Wincoin
English name: WinCoin
English abbreviation: WC
Total issuance: 0.5 billion (0.45 billion is expected to be digged).

BLOCSIZE: 512K
Algorithm validation: POW+POS
Compute mode: POW (Scrypt)/POSV3
Interval of producing block: 60s
The amount of currency produced by each block: 0.01
Interest: 3.5%

6.2 **Allocation of digital assets**



6.3. Interest incentive mechanism of Wincoin

Wincoin adopts the hybrid consensus mechanism of POW+POS, which is verified by double algorithm. The amount o issuance is 0.5 billion, 0.45 billion is expected to be digged, and the other 50 million is the interest bonus to the holders of Wincoin, the interest payment period is three years and the annual interest rate is 3.5%. The holders will obtain more interest bonus if they store more Wincoins.

Concrete implementation method:

①POW: the full name is Proof of Work. POS: the full name is Proof of Stake. The ratio of POW block and POS block is 1:12, which is after each POW block, there can be 12 POS blocks consecutively at most. Wincoin introduces POS, but it doesn't stop POW, the POW is now the

cornerstone, and the POS is the main body. The calculation of the difficulty coefficient of Wincoin is completely based on POW block, POS block doesn't participate in the calculation of difficulty coefficient. POS block also has difficulty requirement, the difficulty is POW standard difficulty / coinage (coinage is the savings days of the amount of currency X)

② The relationship of the calculating of coinage and the interest: there is no new mine in the POS block, it just interest. Establish a system of interest payments based on the amount and time of the currency held. Under POS mode, there is a term called coinage, and each coin produces one coinage per day. Fr example, if you hold 10,000 coins for a total of 10 days, your coinage will be 100,000. If you find a POS block at this time, your coinage will be cleared to zero. If each of your coin has been cleared of 365 coinage, you will obtain the interest of 0.035 coins from the block (it can be understood as an annual interest rate of 3.5%), the daily interest of 10,000 coins =10,000 * 3.5% / 365 = 0.9589 coin, payment time of POS interest coin is irregular, and it is not distributed at a specific time every day, but the the overall number matches.

③ The advantage of the design of Wincoin: the equity holders have the right of control. The purpose of the upper and lower limit design of interest-bearing time limit is to urge the users' enthusiasm on receiving interest and to prevent the user from trying to send the POS block to apply for interest all the time. In terms of security, since PoW only takes effect after been validated by PoS, PoW miners cannot decide and change the rules of the network themselves, which effectively withstood 51% attack.

7. Technology (core) team

(1)Jovian Tan (chief technical officer)

Jovian is the GBBC consultant and has more than six years of experience in the technology industry. He has once been awarded the Hons Degree Of Doctor Of Humanities (PhD) by the All Nation College in Philippines. He graduated from the soft engineering major of the Technical College of Malaysia University (UTM) with excellent academic performance and obtained the full JPA scholarship. He was one of the several applicants in the 600 applicants from southeast Asia who have joined in the Microsoft Academy for College (MACH) program. As the person who helped the preacher of the developer platform, he was given a full-time position to join Microsoft's EPG team of world-class business experts and Windows device business (one of the drive for business). and his task was promote the adoption of the Windows mobile initiative with enterprise mobility. After two years of hard work, he won the FY15Q4 equipment achievement award, one of the only two awards in 2015/2016 (Microsoft FY15). Currently, Jovian is experimenting M2M/ technology of the network of things and Fintech.

(2)WuJun (software engineer)

Wu Jun is graduated from the computer department of Shandong University of Science and Technology, he has 12 years of experience in the network of things, and he is full stack software developing engineer, large network game architect and senior outdoor explorer. He is good at the architecture of the large Internet system distributed server, application of massive database, development of low-level framework and the design and development of sdk and app of the mobile terminal. In 2006, he founded an Internet technology company in Wenzhou, which

specialized in enterprise-level website development and ERP management system. In 2008, he founded a personal studio in Shenzhen, Guangzhou, which focused on network framework development, game engine and data mining algorithm. He has been the technical consultant of several network game companies. He is co-founder of this company, and is good at technical team building and breaking through difficult technical problem.

（3）William (software engineer)

William is graduated from the software engineering of the University of Malaya, and is a senior expert in website software technology. He used to work as a Software engineer at the research and development center of Panasonic for three years and led the team to develop Ants CMS Software. A software for the company to manage the website, Ants is a software whose CMS is built on the basis of SEO and designed and responsive to HTML and other advanced Web Application functions.

(4)Dr. Yu (chief marketing officer)

Dr. Yu is from Malaysia, he is a master of material engineering, and is graduated from Coventry University in England. He has been the manager of the personnel department of an international group and the President of a furniture trading company. And he has an in-depth study on cryptographic digital assets.

8. Reference

1． A. Tapscott, D. Tapscott, How blockchain is changing finance, Harvard Business Review, 2017.

2．T. Stein, Supply chain with blockchain — showcase RFID, Faizod,

2017

3． S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.

4． R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.

5． C. Swedberg, Blockchain secures document authenticity with smartrac's dLoc solution, RFID Journal, 2016.

6．D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.

7． A. Legay, M. Bozga, Formal modeling and analysis of timed systems, Springer International Publishing AG, 2014.

8． A. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.

9 . B. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.

10. KCDSA Task Force Team, The Korean certificate-based digital signature algorithm, IEEE Standard Specifications for Public-Key Cryptography, 1998.