mzcoin

UK mobile digital bank mzcoin digital asset company.

The international whole new fast payment ecosystem.

Content

Chapter one: project vision

Mzcoin is a globally and open whole new fast payment system based on the business application solution of blockchain, tried to develop the smart pay through the establishment of the digital currency pay system on the blockchain, building the whole new ecosystem of payment and connecting global users together. Removing the barrier between users and enterprises development through mzcoin and building the convenient fast pay system based on the decentralization, smart contract, and trust mechanism of blockchain to be the next project with global application scenario and grand ideal blueprint under the guidance of the latest top-level international concept.
The vision of mzcoin is to realize the safe and fast payment through reshape the payment rules of blockchain and mobile payment and enjoy the unprecedented trade experience for global users. As our responsibility, we try to build the creative smart payment to realize the upgrade on the global digital business mode and build the vision of human' beautiful life. The introduction of blockchain, digitization and creative industrial ecology help the development of blockchain technique and application on community service and business growing.

Chapter two: project background

2.1 Innovation of mzcoin.

As the team of the mzcoin project, we have made a lot of innovations on the customer's various needs.

（1）Cluster management

With the increase of the service, the need for the automatic management of lots of servers, separating tasks and breakdown grows as well. Mzconin system includes a great deal of microservices because it will be waste the server a lot if only one task for it. If the classify the servers traditionally, it will enhance the difficulty of service expansion, thereby, a fast payment flexible trunked dispatch system should abstract the operating environment of the application program, isolate the operating environment and basic hardware. Scheduling algorithm make the expansion or reduction according to application load and available resources. Besides, when mzcoin designed the cluster management, it tried to make all the applications in one scheduler, thereby, it could schedule stateless service but also stateful service.

(2) Multilingual service

MZ background system is major coded by go language, because go language has the advantage on coding the low delay and high concurrency program. But only one language is hard to bridge the platform of the whole bank background system due to a lot of potential different coding languages software and the preference of different languages on different technicians. Docker solved the problem on multilingual application deployment, packaging the application and operating environment together, scheduling the system without concerned with the inner actual language. But the code-mixing of many languages will lower the codes on degree of reuse, thereby, it can't extract the common code as the reference of class library anymore.

To solve this problem, MZ exposes lots of basic services through RPC way, transforming "code sharing" into "basic service sharing". For example, if you want to get a distributed lock, it doesn't have to access the etcd through the client, but the RPC interface only. By rpc-making basic services such as databases, message queues, etc., each new language just needs to initiate RPC calls through existing infrastructure services. By this access, MZ completes the compatibility of languages, Java, Python, and Scala, etc.

（3）Remote invocation framework

MZ exposes basic services through RPC, so their infrastructure needs a strong RPC framework to support their microservice architecture. The RPC framework should have the following features: (1) load balancing: most of the HTTP libraries implement polling load balancing based on DNS, but not fluent enough. The ideal load balancing should be able to select the most suitable target server to reduce failure rate and delay. In this way, even if the copies replicated in the cluster due to failure, the performance of the whole system would not be affected.(2) Retry-on-error: for the distributed systems, failures are unavoidable. If an idempotent call fails, the RPC system should be able to automatically request other copies in the cluster to ensure the system is still available in operation when a small number of failed nodes existing in the cluster. (3)Connection pooling: if every request needs to recreate the connection, the delay of remote calls will be greatly increased. Ideally, every remote call request should try to reuse the created connections. (4)Routing: for a RPC system, it is necessary to modify the target machine at runtime. For example, a new version of service on line may need a certain gray level process. From the new limit to 100% use, it is necessary to gradually introduce traffic to the new version service through the routing function.

Based on these characteristics, MZ finally chose Finagle. It has all the characteristics above, and its modularity design also reduces the cost of learning.

(4) Asynchronous message

Most of the business logic of MZ in the background is accomplished through

asynchronous messages. Although some operations take a very short time, asynchronous messages can provide users on task status with faster feedback.
Since large number of core logic has been asynchronous, each message is very important, thereby, each step message of on a complete business operation cannot be skipped, even if an unrecoverable exception occurs, the whole process should be able to continue the execution after troubleshooting. Therefore, for asynchronous messaging architectures, the following characteristics must be met: high availability, scalability, persistence, playback and at least one delivery. Based on the above characteristics, MZ finally chose Kafka after comparing the multiple message middleware, Although Kafka is quite different with general message middleware, it is more like a replicable commit log, its features just meet the requirements of mzcoin for asynchronous messaging architecture. First, the replication and database partitioning characteristics of Kafka can meet the requirements of high availability and scalability. Then, a Kafka user only maintains a cursor in a commit log, which reduces the cost of the publish / subscribe model pattern, and can also rehashed the past messages by the modification of the cursor.
To sum up, with the support of mzcoin, the MZ project has a unique innovation model, strong financial support and strong background strength. The MZ project team can ensure the project continuous running once begins.

2.2 The status of the industry

1) Unbalanced global mobile payment market

The situation of mobile payment in country-by-country is great different. From the overall situation of global mobile payment, the mobile payment in developing country is faster than that in developed countries. Take the world's largest developing country as an example, mobile payment is ahead of the rest of the world, "cashless society" mobile payment era is coming globally, In the developed countries such as the United States, the penetration of mobile payment is not high, most people still use credit card offline shopping, and if you want to use mobile payment, the general fee will be 3% - 5%.

2) High attention on payment experience and fund security

According to the market research, to improve transaction security was always at top during the improvement from global web users on mobile payment in 2016 and 2017.It showed the concerns of uses about their financial security are important factors for the development of mobile payment.

Payment is a real problem for global users, it usually needs to copy and paste the account and search for a forgotten card reader. Based on this, we created mzcoin, to achieve instant payment, that is, point to point payment.

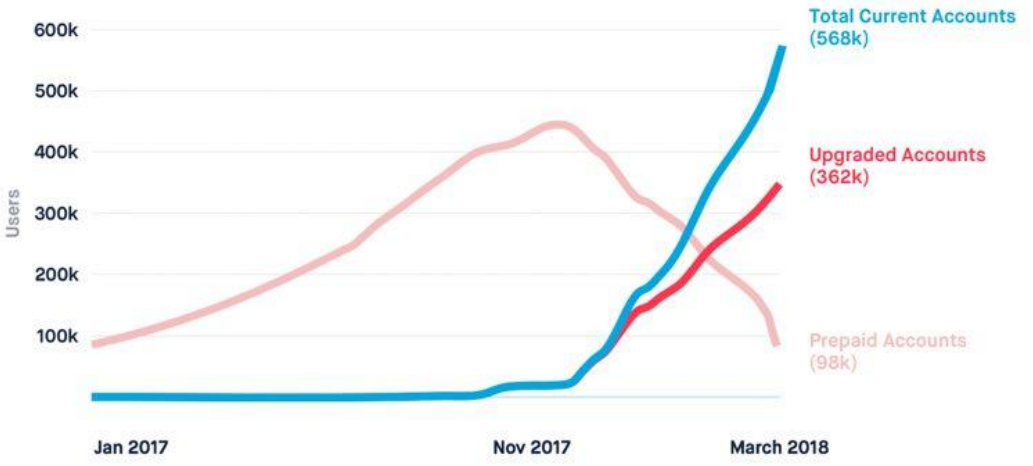


Figure 2-1

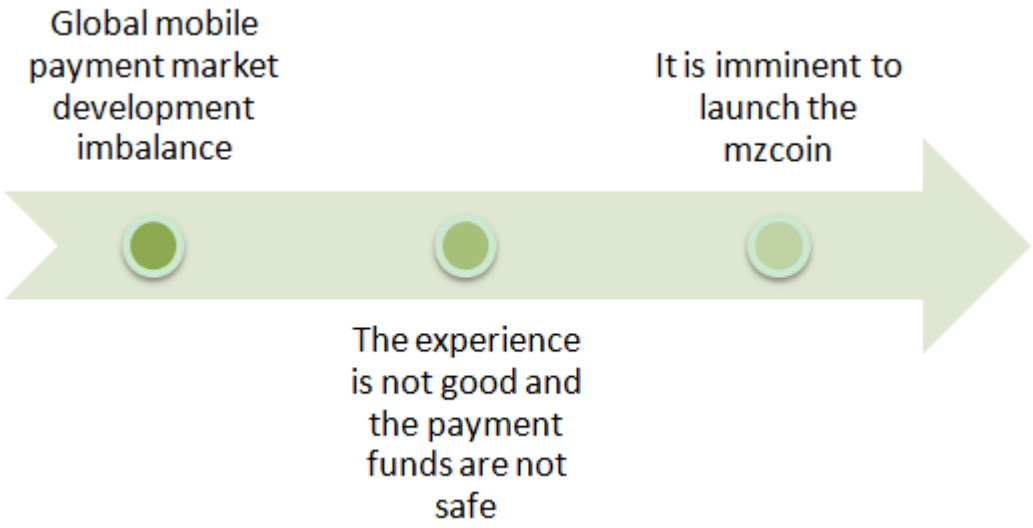


Figure 2-2

2.3 Solution

For a long time, banks have become slow, complex and opaque, and the future of banks lies in immediate inform. Mzcoin wanted to change this situation, and mzcoin tried to make a personal bank for everyone suitable for everyone and every enterprise. By joining our common mzcoin community, many community users can directly express their needs. Users can actually get real-time feedback and program stesting. Through each individual's efforts, we will build a new and perfect new mzcoin ecology.

Mzcoin set up a global fast payment ecosystem to solve the problem. Mzcointried to

create a blockchain technology recording the value of traffic data with the introduction of Smart contracts, building a decentralized mzcoin ecological platform, avoiding the various disadvantages brought by centralization, enhancing the security of payment, protecting the privacy of the users, enhancing the credibility of the data, and eliminating the phenomenon of private tampering or destruction on data to establish a safe and credible platform mechanism for users.

By allowing users to hold MZ in the ecosystem based on blockchains and smart contracts, it can be driven to pay and cooperate for users in the ecosystem. By holding MZ, users could enjoy the services from various alliance enterprises cooperating with mzcoin. Users can trade with MZ or convert into legal tender. At the same time, when more users join the mzcoin eco platform, the MZ will increase its value because of higher scarcity. In this way, an open, fair, democratic smart payment ecosystem with most user participation and user sticky has been created.

The third chapter: Introduction of the project

3.1 Definition of contract payment

Mzcoin is not only the same as bitcoin, but also ae-commerce contract payment system based on blockchain payment system. Users sign the contract among them through the private key to complete the MZ payment transaction. In fact, mzcoin can be used to sign any MZ contract. If the contract connected with a digital asset registered on the mzcoin blockchain, then mzcoin can automatically carry out the procedural delivery on the chain; if the contract connected with the asset outside the chain, the contract participant can execute it by itself. Even in the latter case, mzcoin has eliminated the tediousness of signing and keeping a large number of paper contracts, and guaranteed the non-repudiation of the contract with digital signatures. Through the contract payment mode, a perfect credible mechanism has been established, and the revolutionary development of smart payment has been promoted.

3.2 The matching between foreign trade finance and blockchain

Foreign trade finance and blockchain technology have enough "collaboration space". The connection between foreign trade finance and the blockchain created a distributed and non tamper-resistant payment community using the new encryption authentication technology and decentralized mechanism, the MZ issued digital currency will connect all the users continually.

Blockchain is an innovative application mode of computer technology with distributed data storage, point to point transmission, consensus mechanism, encryption algorithm, etc, in the Internet era. This technology is a subversive innovation mode after personal computer and the Internet, highly likely to cause a worldwide new technological innovation and industrial transformation. We can also consider blockchains to be a machine that makes trust, because blockchains can generate a set of chronological, tamper-resistant, trustworthy databases.

The management application of blockchain on foreign trade finance is matured development operation of blockchain technology. The birth of blockchain marks the beginning of the construction of a truly trustworthy Internet. It is shown that the concerned point of blockchain is about the establishment of a reliable trust between point to point through analysis of the development of the blockchain which eliminated the interference of intermediary in the process of value transfer, both public information and privacy protection, both decision-making and protection of individual rights and interests, this mechanism increases the efficiency of value exchange and lower cost. Smart contracts make use of the tamper-resist of blockchains, and perform predetermined contract contents when they are triggered, and different people will get the same results in the same smart contract, thereby eliminating differences and creating a mutual trust platform. At present, a single independent blockchain system has a far-reaching effect on earth, and we believe, as a chain routing system, it will improve the commercial value of the blockchain system.

Mzcoin created a new distributed chain smart payment system with this faith. Mzcoin tried to popularize the product to all users, so that the different industries can enjoy the convenient and safe services brought by the MZcoin, and protecting the development of human beings.

3.3 What is "mzcoin"

Mzcoin is built by the world's top 50 bank-Britain's Lin Dun mzcoin project team, the global first smart payment system based on blockchain and smart contract, and decentralized intelligent trading system, with the help of the fairness and openness, it made global transactions more secure to build a huge, stable, transparent and convenient payment ecology.

The vision of mzcoin is to create a global mobile smart payment system and build a mzcoin ecosystem. In our distributed partner alliance, it used the digital encrypted virtual currency designed for security transactions to provide services to various forms of organization in different cultures, different countries and different languages, based on an open environment and connected the real world with the digital world ,creating a technology based and trusted trading environment.

In mzcoin, we used the micro services architecture and divided the code into many tiny and independent parts, which makes the code easier to develop and run reliably.

In this way, mzcoin implementation the pattern of p2p-payments.

In addition to introducing the payment currency on mobile smart payment, mzcoin is further collaborating with various industries to build a global application ecosystem of "blockchain + payment + industry + consumption".

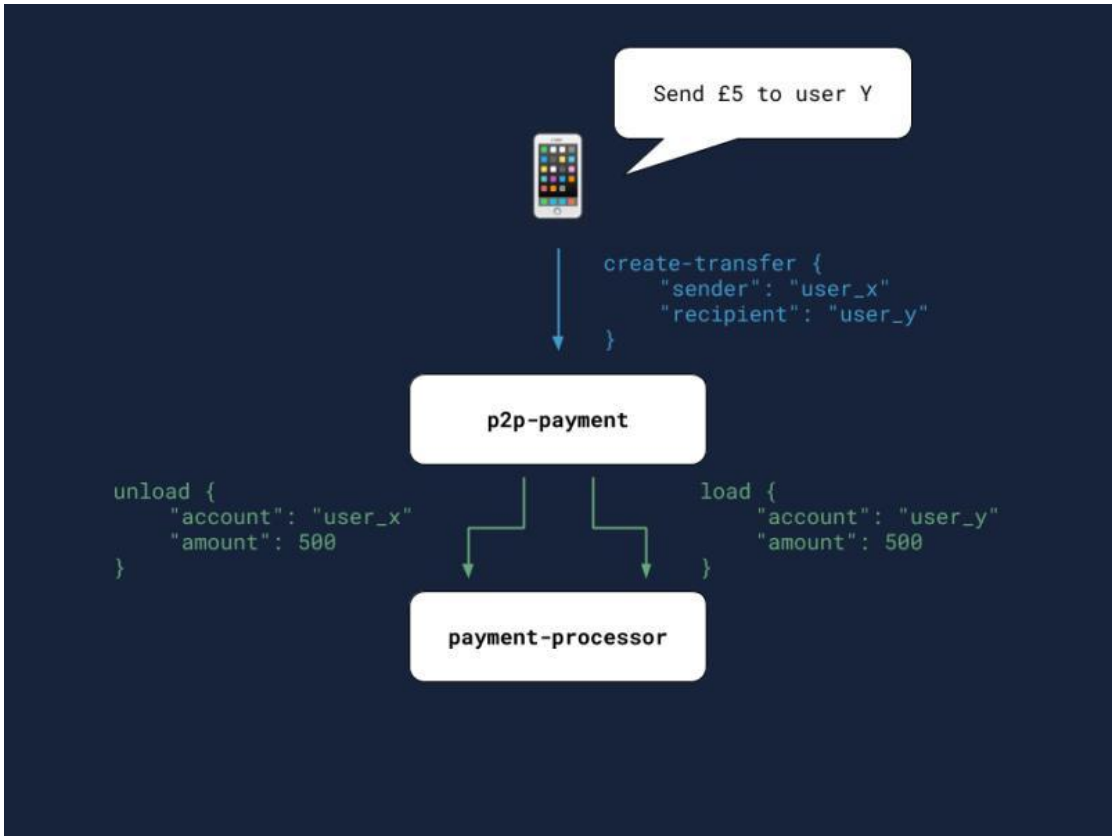


Figure 3-1

3.4 Innovation of mzcoin

1) Further decentralization

Based on the PoW consensus mechanism blockchain, it required a third party to provide the corresponding calculation force to pack all the transactions, who has the power to charge and to choose the packing, thus a large number of mines with centralized computing power have emerged. In the blockchain industry, many types of attacks are aimed at the mine because the computing power of the blockchain has been concentrated to a certain extent. However, there is no centralized mining in the network system of DAG, and mutual authentication among users has made it further decentralized system.

The PoC mechanism used in the mzcoin verification process can also effectively balance the whole network. Just more computing power is not enough to make a user

node master absolute power in the whole network. Only the contribution of the network can make the node have more returns, and his contribution is reflected by the service and convenience of other user online.

In the mzcoin platform, the blockchain technology makes many alliance enterprises a distributed alliance based on the decentralized model, and it can form a sustainable, open, transparent, non-centralization, safe and reliable, open and common cooperative ecological platform.

2) The interaction of smart contracts

"Cross chain" has always been an important issue in the development of blockchain. Its meaning is to realize possible interconnection with all kinds of chain structures to better realize their own network value. The DAG architecture of mzcoin itself is a network structure, and the so-called "cross chain" implementation is only the interaction between simple smart contracts. The time stamp and the direct parents we propose are the important technical and logical guarantee of the new interactive intelligent contract.

The mzcoin platform will provide the user with a rich enough smart contract template to facilitate the allocation and automatic execution of MZ and open ports, allowing all people in the ecosystem to participate in the design and distribution of smart contract templates, also to define their own price or incentive conditions same as the founding team, obtaining the corresponding MZ incentive through the usage of users, that is, the unused smart contract template can’t get income, even the founding team and the alliance itself.

3) Improvement on the transaction speed

For the current blockchain technology, the trade speed and the trade volume in whole network are limited by design problems, the speed of block packing and the capacity of blockchain set the threshold for the speed and the volume. More users led to the more congestion of network. In addition, theoretically, the performance of miners is proportional to the number of transactions in the whole network.

The difference in mzcoin is the user helps the user to confirm the transaction, and the transaction unit links together, more and more users and larger and larger volume of transactions led to faster the transaction speed in the network. Theoretically, there is no clear bottleneck in our transaction concurrency.

(4) More secure on user privacy

Mzcoin has a unique privacy protection encryption contract, that is, the original data of privacy can be completely isolated to access through secure multi-party computing to implement a fast and secure data sharing service. The data can be stored in the decentralized resource through the blockchain encryption, authentication and its mechanism, etc. No organization and individual can touch the user's original data except for user itself. The data can be limited to use only by users' consent and

authorization. Under the cryptology's differential privacy encryption, the application can carry on large data on the user's part data, but it can't parse the personal data, view, copy or tamper with the data.

5) A safer, more convenient, and faster transaction experience

The distributed exchange in mzcoin provides a decentralized deal to avoid the loss of data and the loss caused by tampering. Electronic contract transactions guaranteed the security of the user's assets and brought a more secure and convenient transaction experience.

As the central currency of the whole alliance ecology, mzcoin connected the trading, exchange and circulation channels with other coins (other digital currencies, legal tender and digital assets) working as a lubricant that runs through the whole ecology, with immeasurable personal value.

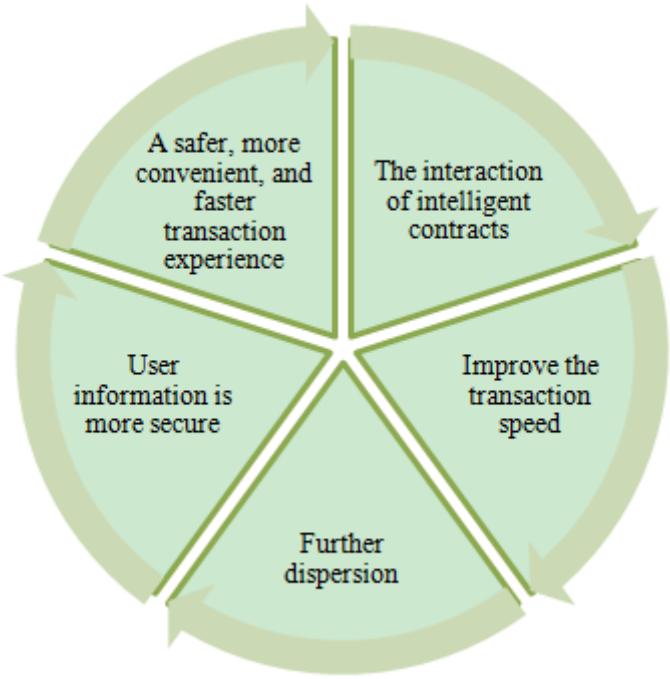


Figure 3-2 Innovation of the mzcoin

Chapter four: overall structure

4.1 Ecological structure

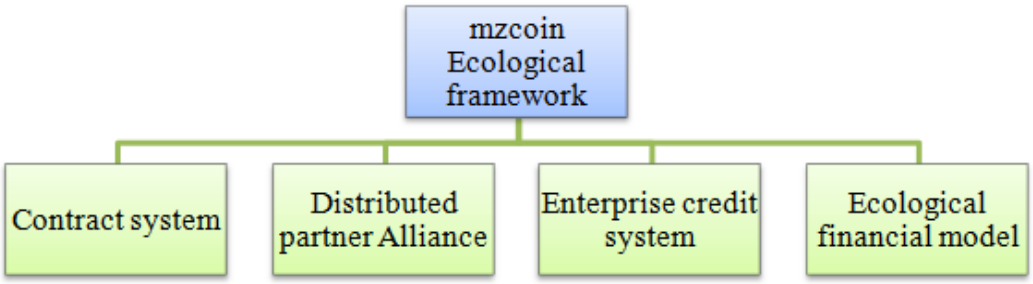


Figure 4-1 Mzcoin ecological architecture

4.2 Contract system

Blockchains have been used to consolidate contracts between enterprises, and neither side can change the terms.

In smart payment, smart contracts have huge space. All transaction data of the user will be recorded in one block, and the agreements signed by the corresponding enterprise can be kept permanently, without any doubt or hidden expenses. One of the typical services offered by mzcoin is to provide a variety of smart contracts.The various products and services of the MZ transaction requires using the smart contracts provided by mzcoin (but it is important to note that the design of smart contracts is not only provided by the mzcoin team, any user in the platform can design an smart contract, " The users can obtain MZ once their contracts were used. Smart contract has the characteristics of tamper-resist, which can protect the security of transactions.

4.3 Distributed partner Alliance

The mzcoin platform will attract the vast number of partners to form an ecological alliance to integrate clothing, food, housing, travel, tourism, entertainment and human life. Mzcoin recruited partners in the world to realize the establishment of the global system of ecological chain. By using MZ, users can integrate daily life and entertainment together, greatly improving the user experience. Thus, as a virtuous cycle, a smart win-win payment ecosystem also mutual benefit was born.

4.4 Enterprise credit system

Mzcoin used blockchain technology to establish an enterprise credit system, collecting a series of behavior of the users in the platform, carrying outdata analysis, forming the user final credit report to provide credit service for the global financial institutions.

The enterprise credit system of mzcoin included six types of data: user basic information, user behavior, user consumption ability, user financial ability, user loan information and user asset information, covering all round, accurate, with very strong usefulness, operability and applicability.

(1) User basic information

The content contained in the user's basic information of the credit report, in accordance with the thirty-third provisions of "financial institutioncustomer identification, identity data and the management methods for the preservation of transaction records", is that the "basic information" of a natural person's customer includes the name, sex, nationality, occupation, place of residence or address of work, contact way, the type, number and expiration date of the identity document or the identification document. If the place of person residence is inconsistent with the place of habitual residence, he needs register the place of habitual residence. The "basic information" of person foe legal persons, other organizations and individual business households includes the name, domicile, business scope, organization code, and tax registration number of the person, which can prove the name, number and validity of the license, certificate or document of the customer in accordance with the law,the type, number and time limit of the name, identity certificate or identification document of the controlling shareholder or the actual controller, the legal representative, the person in charge and the authorized handling personnel.

(2) User behavior

The analysis report on user behavior mainly included the following data: the source area of the user, the domain name and the page, the user's stay time, the rate of jump, the return visitor, the new visitor, the number of return visits, the number of visits and the number of visits, and the analysis of the browsing habit between the users and the non register users; search engines, keywords, associated keywords and key words used by the user; chosen type of entry form (advertising or site entrance links) is more effective; the user visits the site process to analyze the page structure design reasonable or not; the user's web page hotspots distributed data and page coverage data, visitor volume at different times, user preferences for font colors of the website, etc.

3) User consumption ability

User's consumption analysis report includes user's natural consumption, social consumption power, absolute consumption power and consumption ability of

knowledge and skills. Natural consumption is a inherent ability to consume material of people, growing with social and economic development, but its basic attributes are determined by human physiological function, different physiological functions decided different natural consumption power, and absolute consumption power is the ability to consume material of cultural life after production develops to a certain level. The difference between natural consumption power mainly lies in the natural consumption force emphasizing the limitation of physiological function while absolute consumption emphasizing the limit of production and development level and social progress, also including spiritual and cultural aspects. Social consumption power is the consumption capacity restricted by the distribution relationship on the basis of production development. In general, the social consumption power is less than the absolute consumption power while the consumption ability of knowledge and skill in the sense are the condition or means of consumption, sometimes referred to the consumption power.

(4) Financial capability of user

The analysis report of the user's financial ability mainly includes the following two aspects. On one side, it is the relevant knowledge on the user's financial aspects, such as the portfolio management of risk assets, the basic analysis of the stock and the means of technical analysis, the knowledge of accounting and law etc. On the other side, the financial investment situation of the users, for example, the user belongs to the prudent financial management or the radical financing; the users prefer the low income low risk investment of the fund or the high yield and high risk investment, such as the bank deposit or the stock bond.

(5) User loan information

The user loan information analysis report mainly includes the loan situation of the user (enterprise user, individual user) in the bank and other financial institutions (including the loan amount, the loan risk category, etc.), the repayment situation (including the repayment period, the amount of the repayment, etc.), the performance situation, and whether there is any misconduct or not. In addition, it also pays attention to the loan information of users using all kinds of fund-raising websites on the Internet.

(6) User asset information

The analysis report of user assets information mainly uses large data to analyze the user's money information, stock and other securities information, fixed assets information and patents and other intangible assets information. By reporting user assets information, financial institutions can help users to judge their own strength and user's ability to perform.

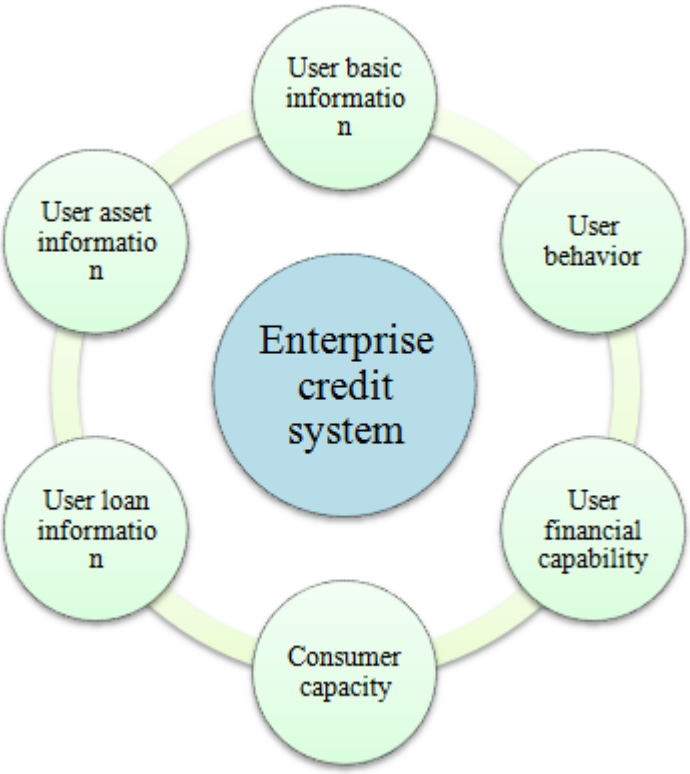


Figure 4-2 Corporate credit system

Compared with the traditional mobile payment system, mzcoin combines the payment with the blockchain to create a new eco-finance mode that belongs to the whole mankind. Mzcoin, as a fast payment system, is a new digital currency bank. We aim to reshape the state of payment in the financial field, promote the development of ecological finance, and further promote the development of the digital world. It is a bridge to connect the virtual world to the real world, to promote the emergence of a unique digital world, and to become the medium of individual information transmission and value exchange in the real world.

The fifth chapter: the application and value of mzcoin

5.1Mzcoin application scene

Mzcoin's application scene is very rich, covering all aspects of life, clothing, food and housing and travel, etc. The introduction of mzcoin's multiple payment solutions, life service solutions and public service solutions can penetrate the mzcoin into people's lives. By building the bridge of "real world - blockchain world - real world", mzcoin is applied to traditional small frequency high frequency scenes such as retail, catering,

business super and logistics, and new applications such as hospitals, ticketing, entertainment and transportation.

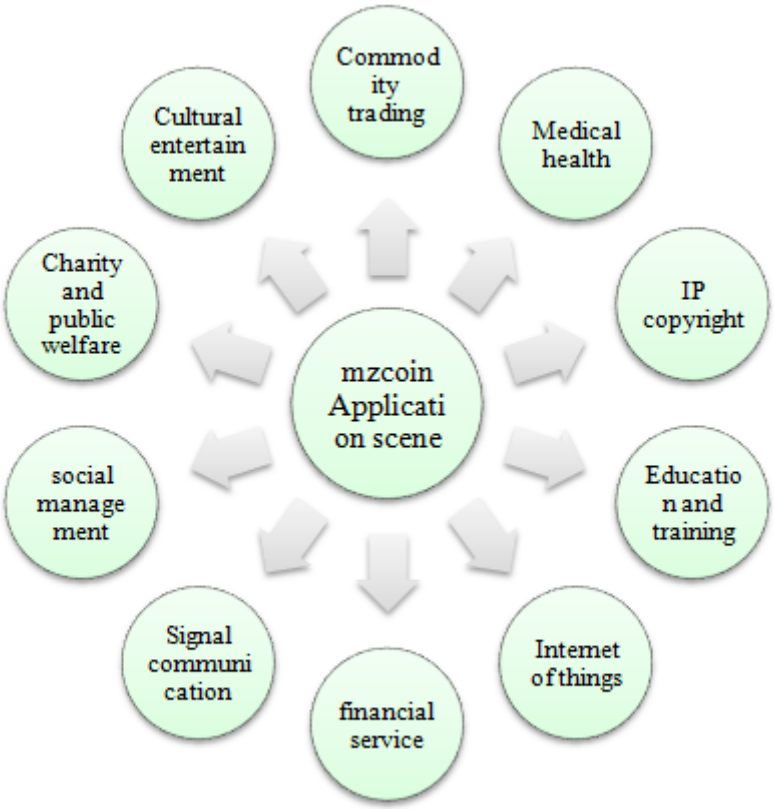


图 5-1 Mzcoin application scenario

5.2 Future application value analysis

With the rapid development of the social economy, the traditional Centralization Payment Mode has appeared a lot of disadvantages. The distributed payment mode that seeks security, efficiency, encryption and cooperation gradually reveals its strength. The corresponding distributed technology is also able to obtain the development space, and as a whole new distributed infrastructure and calculation method. Blockchain technology has also attracted wide attention in recent years. As the forerunner of blockchain exploration, mzcoin has gradually realized the application of blockchain technology. Mzcoin vigorously promote the application of the payment currency scene, give full play to the advantages of the central feature of the blockchain technology, the advantage of tamper-resist, the mutual trust consensus, the intelligent contract, the traceability and the audit, constantly promote the application of the block chain technology.

Mzcoin intends to lead a number of member agencies to build a world-class distributed payment system, and constantly promote the formation of the blockchain ecosystem. As the world's first and the world's leading payment mode, mzcoin helps

to solve the security problems of mobile payment and the low efficiency of credit card payment. It also makes a unique contribution to the open source and application of blockchain technology in the field of payment. According to the requirements or conditions of special business needs, existing technical level and laws and regulations, mzcoin comprehensively optimized from various fields, such as business safety, performance, cost, policy, technical feasibility, operation and maintenance, and management, which provided an opportunity for future development.

Chapter 6: block chain application

6.1 Infrastructure overview

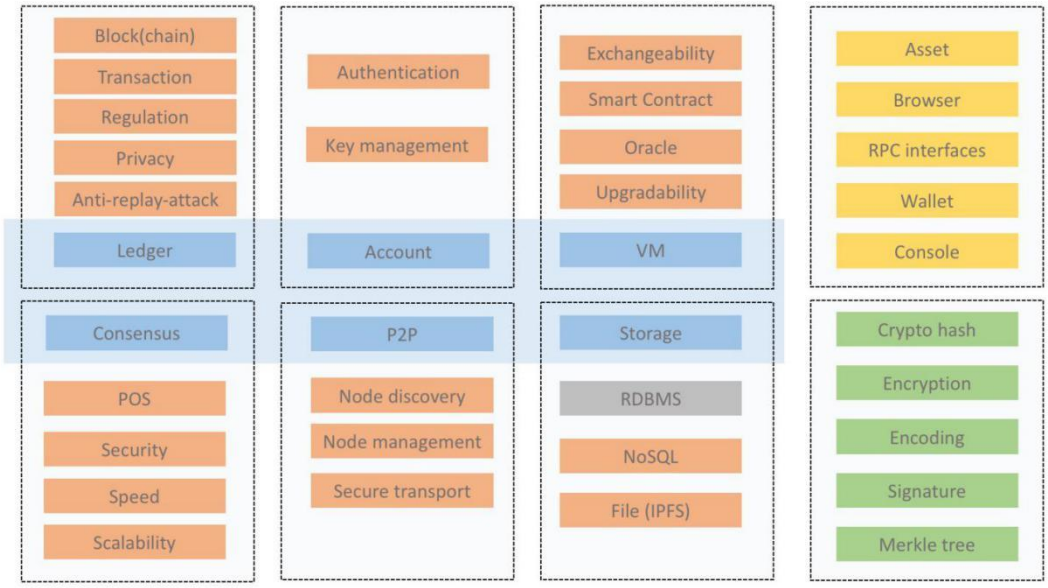


Figure 6-1 Mzcoin blockchain infrastructure

6.2 Development service layer

6.2.1 Smart contract life cycle management

a) Allows developers to design and create smart contracts that contain business logic. Business service systems interact with blockchain systems through interfaces and other interaction mechanisms.

b) Provides lifecycle management functions for smart contracts, such as creation, calling, upgrading, and destruction.

c) Provides upgrades and data migration capabilities for smart contracts, but it has to

meet the upgrade rules of the original smart contract settings.

6.2.2 Smart contract combination service

a) Recreates new service functions by combining one or more smart contracts.

b) Design an integrated interface for service users to access multiple blockchain system service functions.

6.2.3 Smart contract testing service

a) Test the component functions implemented in the blockchain system to ensure that these components complete and correctly implement the service function.

b) Tests the component functions implemented in the block chain system to detect the security and robustness of these components.

c) Ensure the interoperability of service function interfaces.

d) The test should cover the service deployment nodes in the blockchain system.

6.2.4 Smart contract template service

a) Mzcoin system adopted the current mainstream virtual machine mechanism in the chain business, currently supporting the EVM virtual machine compatible with the ether Fang, which can directly deploy and run the solidity smart contract. It is also actively developing more virtual machines closer to net red economic applications, and facilitating the rapid development and customization of business logic in the chain.

b) Predefined contract modules: it can use blockchain system quickly. For some common business scenarios, the mzcoin system has developed a number of directly used chain business contracts (such as integral chains). The group can directly choose deployment / use according to the actual needs.

6.3 User service layer

6.3.1 Purse

Users can create their own public and private key accounts through their purse, also can conduct several gold coins transactions and smart contract calls, etc. through their purse.

6.3.2 Account

Accounts are essential for users to interact through the chain of transactions and Ethernet blocks. Accounts represent the external agents identity (such as personas, mining nodes, automatic agents). The account used the public key to encrypt the image signing the transaction so that the Ethernet virtual machine can authenticate the sender's identity safely. Each account is defined by a pair of keys, a private key and a

public key. The account is indexed by the address, and the address is derived from the public key, taking the last 20 bytes. Each pair of private keys / addresses is encoded in a key file. The key file is JSON text file can be opened and browsed in any text editor. The essential part of the key file is the account private key, usually encrypted with the password set up when you create the account. The key file can be found in the keystore subdirectory of the data directory in the Ethernet node.

6.3.3 Storage

Mzcoin contains two aspects of the external storage module. IPFS is used to store large files outside the chain, while structured storage is used to save structured records and support structured query languages.

IPFS module: mzcoin introduces IPFS technology to support large file storage. Through hash storage, the file has the characteristics of tamper-resist, never losing, leakage prevention and access security, avoiding the impact of accidents on data security, ensuring the permanent preservation of relevant information, ensuring data security and user privacy cannot be leaked and lost.

Structured storage module: structured storage is used to preserve structured records and keep track of records on blockchains.

6.3.4 Privacy protection

The privacy module provides cryptographic contract related services and various privacy solutions.

Encryption contract: provides an encryption contract solution for smart contracts with privacy requirements. In the encryption contract, the information in the smart contract and the transaction of the contract are encrypted. The private transaction adopted the method of local consensus, and the execution of a private transaction is divided into two steps: the first step is the preprocessing, the private transaction is converted into a common transaction [S1=>S2] (S1 and S2 are the cipher text states of the smart contracts before and after the transaction execution, respectively); the second step is to pack [S1=>S2] as a common transaction into the block.

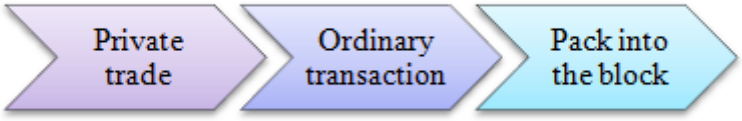


Figure 6-2

Privacy solution: mzcoin provided different privacy solutions for different scenarios, such as multiparty computation and PGP communication. Through secure multi-party computation, mzcoin can achieve completely isolated access to raw data of privacy. The PGP security communication solution provides a fast and secure data sharing

service for mzcoin.

6.4 Blockchain bottom service

6.4.1 Security mechanism

Select the encryption mechanism that conformed to the international standard, encrypt the data in the chain, the transaction data between the users and the users with the corresponding rights of the traders and owners can be viewed.

6.4.2 Consensus mechanism

The value anchor of the blockchain lied in the consumption and output of the chain itself. When the blockchain selects PoW (Power-of-Work, workload proof) as the consensus mechanism, the generating cost of each block will become the cornerstone of its value. In addition, on the mzcoin, each node has the ability to solve the real environmental problems, and provide various services to the outside world. If every node on the mzcoin can participate in the settlement of shared work, the entire blockchain will have realistic output value. Therefore, in order to maximize the value of the blockchain, mzcoin will choose the consensus mechanism based on PoW automatically. The core meaning of PoW is: the greater the computing power, the greater the probability of digging into blocks, the greater the weight of maintenance blockchain security.

However, because PoW has the dominant defect such as slow transaction speed and so on, the consensus mechanism of the follow-up data chain in the platform will be designed to be modular, and can be configured through the control chain parameters, and can dynamically apply the different application scenarios of the public chain and the private chain. The mzcoin platform will choose suitable consensus mechanism for the application scenarios of the data link itself to ensure that the data consistency of the distributed nodes is achieved through the algorithm.

6.4.3 Cross chain communication protocol (CBCP)

The communication protocol between blockchains is similar to TCP/IP protocol in traditional networks. Messages are divided into two parts: message header (Header) and communication information (Data). The message header will record the source, destination, length and category of the message. In the process of transmission, the header will be stripped and modified, and the information will be transmitted to the destination of the message. In addition, message transmission is stateful. The sender can understand the state of the current communication according to the feedback of the receiver and make the correct response.

1) Protocol structure

A complete cross link communication protocol (Cross Block chain Communication Protocol) mainly consists of two parts, communication address and communication

package.

The communication address includes the chain identifier (fromChainID) of the message source chain and the current chain height (Height). The communication package is composed of parts, communication Baotou (Header) and communication information (Data). Among them, communication Baotou includes the starting chain identification (srcChainID), the target chain identification (dstChainID), the communication state (Status), the time-to-live (TTL), and the trigger communication transaction. Communication information will not be opened in the process of transmission.

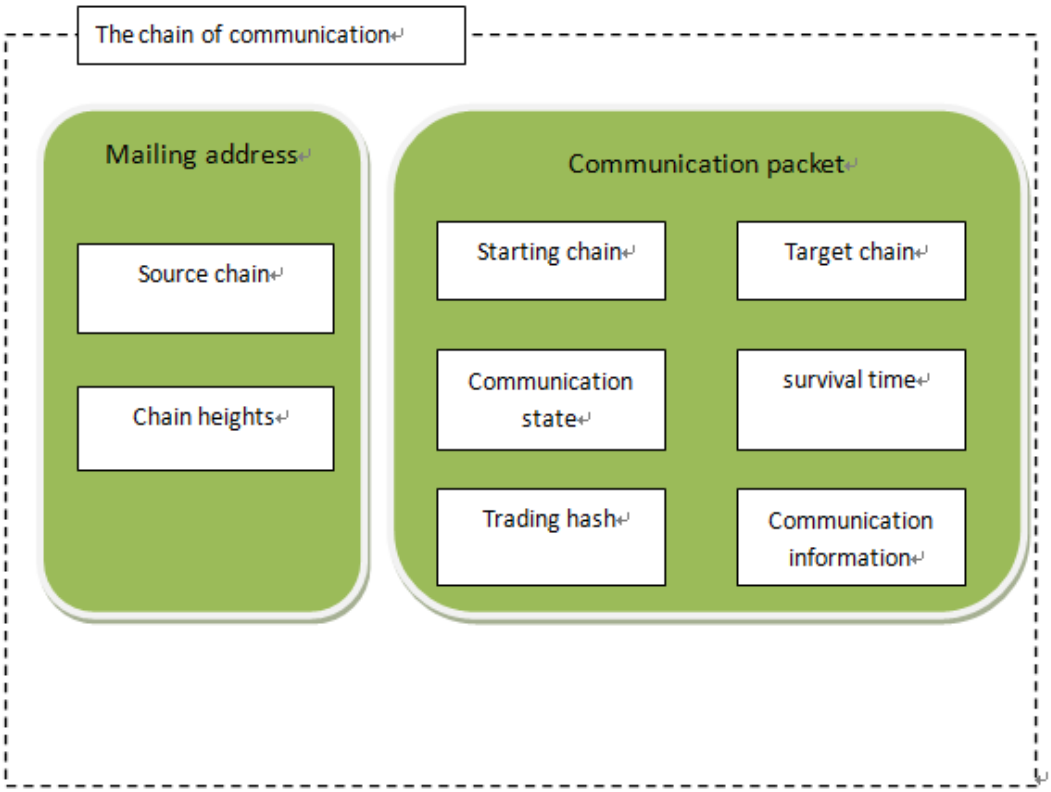


Figure 6-3

The communication state corresponded to the state mechanism in the network protocol. When a communication package is sent, the communication state is "received and peding". When the receiver got the message, it returned to the sender a communication package in which the communication state is "sending success". If the sender receives a communication package containing the "send success" identity, the sender will return to the other party a packet containing the "receive success" identity. The above is a successful communication. If the package reception failed in the process, for example, the recipient does not reply to the "send success", the sender will reissue the transaction after a certain time and try to establish the communication again.

In addition to the above state, we also specify the "connection timeout" state. When a

transaction is sent from subchain 1 to sub chain 2, it specifies its assigned communication survival time based on the height of the chain routing block. Before the communication survival time is reached, the chain route will return the state of the result of the communication to the subchain. If the communication survival time is exceeded, the chain route returns directly to the sender "connection timeout" state. The sending subchain records the communication as a communication failure.

2) Communication verification

Similar to network communication, block cross link communication may also be attacked, especially DDoS attacks. Therefore, we need a set of communication verification mechanisms that are easy to verify and forgery to prevent chain routing from being attacked.

The structure of chain routing mentioned before is a standard structure that the subchain should be consistent with in our opinion. Under the framework of standard structure, chain routing will make it easier to verify communication requests from subchains. As mentioned above, the subchain sends the latest block and commit to vote (Commit). When a transaction comes from a subchain to the chain route, the exchange is shown in the communication address to the height of the block. We only need to find out if there is any transaction in the block at that height. Because by submitting the latest block and its voting (Commit), it is enough to prove the authenticity of a block. The proof is below:

First of all, relying solely on a block cannot prove its legality alone. Because for an existing block, we can fake a counterfeiting block with block structure in line. For example, modify transactions in block data parts and modify transaction hash values in zone blocks.

A block was proposed after two rounds of voting, in which second consensus ballots were temporarily saved and considered as part of the next block of blocks. Based on this, if the subchain is submitted to a block and its voting at a time, we can prove the credibility of the block in a round block generation time. Instead of spending the generation of two blocks, waiting for the next block to generate, and verifying the reliability of the previous block by the authentication part of the previous block.

The process of verifying the legitimacy of an independent block through consensus is that the block is not tampered with the data in there and the hash value of the voting part to verify that. Because the Commit is the signature of the chain over the block area the 2/3 authentication node, unless the sender of the message can simultaneously control the private key of the authenticator on the chain over 2/3, no one can forge a block.

6.4.4 Rights and interests management

Each participant holding Token has the opportunity to become a verification node, and the verification node must be mortgaged to the shared fund pool, and the verification node vote weight is calculated according to the proportion of its mortgaged tokens.

When the total number of verification nodes is not up to the upper limit, each token holder can apply to be a verification node, and when the number of verification nodes has reached the upper limit, the non verifying node wants to be a verification node, the number of the token must be greater than the amount of the minimum weight of the current verification node. A non-verification node with fewer token amounts can also delegate tokens to a representative, who can distribute prizes proportionately to these consignors. In this way, participants with less token can also join the consensus through finding agents, and reduce the losses caused by the annual inflation of the tokens.

Chapter 7: mzcoin system

7.1 Character of real right

In the designed ecosphere, the users with MZ tokens have the ownership and disposal of MZ tokens, that is, the property of the MZ, and can dispose of MZ arbitrarily within the scope of the law. When the user obtains some goods or services in the mzcoin alliance enterprise through the disposal of MZ, it obtains the ownership and the right to use the products purchased by the accepted service.

In the platform, all transactions need to be carried out through MZ tokens, and users need to exchange production, material, and life information, etc. with others through the MZ token. The transactions give the attribute of MZ currency, that is, MZ token is a right, which has the right of value, circulation, storage and payment. In addition, the MZ token is an encrypted digital asset that is the product of the international encrypted digital currency / blockchain community, which can be verified, traded, and exchanged anytime and anywhere.

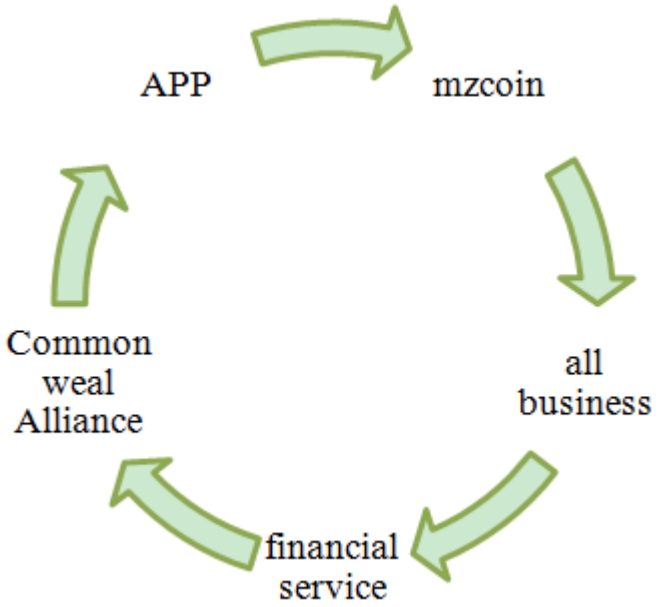
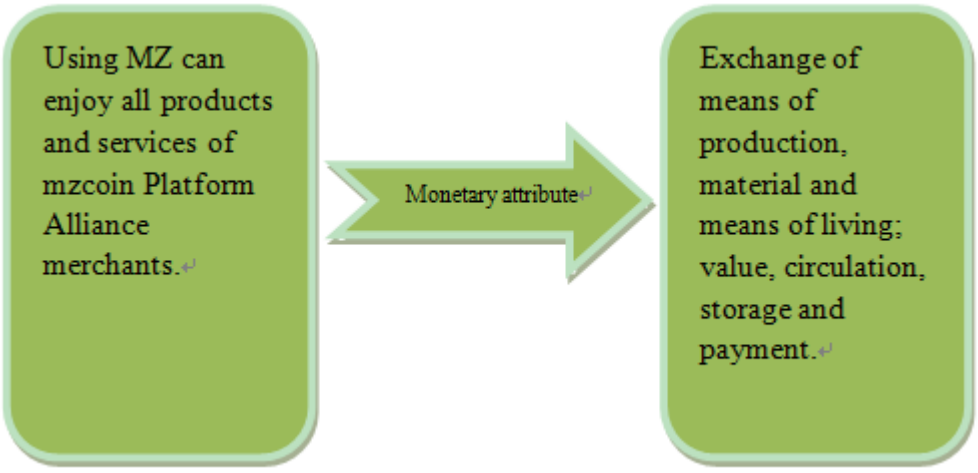


Figure 7-1 Mzcoin property.

7.2 Monetary attribute

In the platform, all transactions need to be carried out through MZ tokens, and users need to exchange production, material, and life information, etc. with others through the MZ token. The transactions give the attribute of MZ currency, that is, MZ token is a right, which has the right of value, circulation, storage and payment. In addition, theMZ token is an encrypted digital asset that is the product of the international encrypted digital currency / blockchain community, which can be verified, traded, andexchanged anytime and anywhere.



7.2 Monetary attribute

7.3 Equity property

The core concept of Token's economic design is to intensify the dissipative transaction costs in the original system, and to disperse the income to every participant in the system by technical means, making the overall friction of the system declining, thus the intrinsic value of the tokens is rising.

The MZ token is the foundation of the application platform operation. The total amount of MZ tokens is not infinite. The total amount of the token is relatively limited. In the long run, greater business of the platform, more users, merchants, traders and investors in the platform, more large users and trading varieties on the platform, more application resources calls, the greater the demand for the MZ tokens higher its scarcity, then, the price of the MZ token in circulation will be higher. This is the ownership attribute of MZ token, and long-term holding can realize value added.

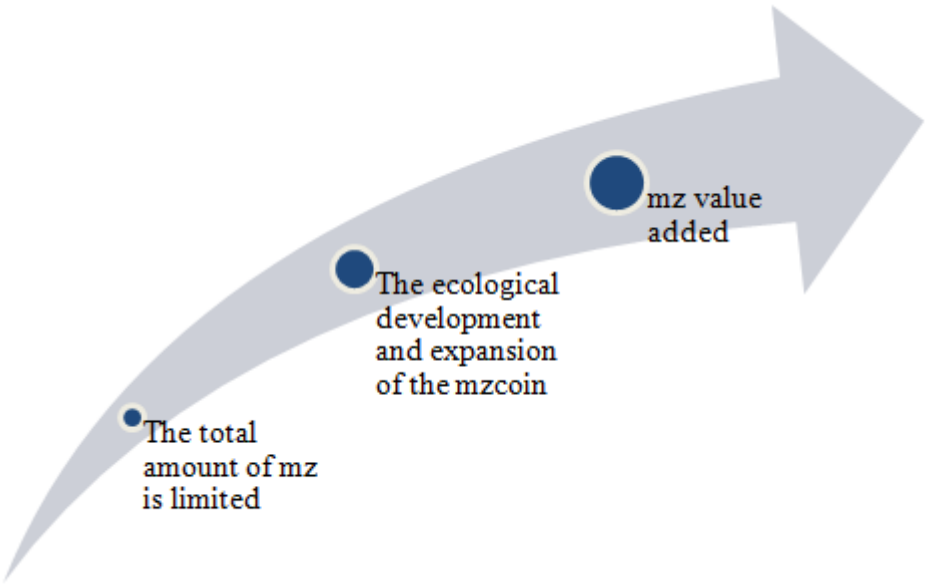


Figure 7-3 Mzcoin equity interest

7.4 Decentralized governance mode

As a global distributed digital currency ecosystem based on blockchain technology, mz is a significant feature of decentralization.

In the decentralized governance model, any decision to complete a vote within a fixed time period varies depending on the proposed content. When only if a high enough vote is collected, the proposal will be implemented, otherwise the proposal will be closed. In decentralized autonomous systems, it is not controlled by the high rights users and the lower rights users could make an alliance against the high rights users.

Decentralization of autonomy includes but is not limited to user registration, statistical functions, and the range of mortgage marks, etc. These upgrades can be determined through the participation of autonomous system.

Chapter 8: Mzcoin realizes development planning

8.1 Initial planning: platform construction

Mzcoin team is gradually building the global ecosystem pay mode, but the team belongs to London, so the team planed to take advantage of the company's natural resources, project early selection in mzcoin covered in Europe.

We adopted the model of big data and blockchain, building a world-class distributed digital money ecosystem, and establishing a convenient, comfortable and safe consumer payment system. Mzcoin planed to help users enjoy more convenient and secure trading services by relying on data mining analysis and machine learning technology.

Our preliminary work is focused on completing mzcoin project launch and the sale of the mz, so it must be a lot of research and exploration, based on the research of the theory of technology, completing mzcoin platform construction and operation.

8.2 Medium-term plan: promotion optimization

After the completion of the mzcoin evaluation, it is necessary to carry out the promotion of mzcoin, such as expanding the influence of mzcoin through baidu promotion, etc.improving the digital trading system and promoting it continuously; This paper discusses the application of artificial intelligence in the platform and subsystems, and the selection of the artificial intelligence.

We will contact more global blockchain exchanges, actively promote the online plan of payment in the world, and enhance the international influence of the mzcoin project. After exchange online mzcoin team and board of directors will persist in the depth development of chain technology, full launch and vigorously promoting artificial intelligence services, and continuously more access to the user and enterprise organization

8.3 Future planning: globalization development

The concept of blockchain was first introduced by European and American countries and established a mature regulatory system and application mode with the development of the market. In addition, as the most developed country in the field of payment, the world has great demand for security payment. Therefore, mzcoin will actively layout the us, global and other global markets after completing the project trial operation in Europe.

In the future, we will recruit partners around the world to realize the establishment of the global ecological chain payment system of mzcoin. Through our efforts, we will use mzcoin to pay for the collection of more than 1,000 enterprises around the world, which will bring the most convenient and safe services to global users and increase the viscosity of the global users to the ecosystem. In addition, mzcoin will have access to multiple applications, organize multi-language platforms, carry out the coordinated operation of global industrial ecology, and create a global ecological circle of a trillion level.

Chapter 9: Mzcoin profit model

9.1 Settlement fee

For mzcoin, settlement fee is its main profit model. The platform will charge a settlement fee of 0.5% to 1% when each stakeholder uses the mzcoin platform trading,. Although settlement fees are very low, the fees they generate can be substantial when transactions are frequent throughout the currency market. The scarcity value of the tokens will inevitably increase more appreciation after more stakeholders pour into the platform to replace the coin, because of the constant total amount of the tokens.

9.2 Financial profit model

Mzcoin provides a new type of financial system, in our platform, not only can be used to pay, also includes financial investment, such as introducing third-party financial products into platform, including all kinds of company funds, loans, etc., providing users with investment service. But not all of these services are free, may charge certain intermediary service platform as the basis of user investment financing costs, this is similar to the stock market in the securities distribution fee charged by the stock exchange.

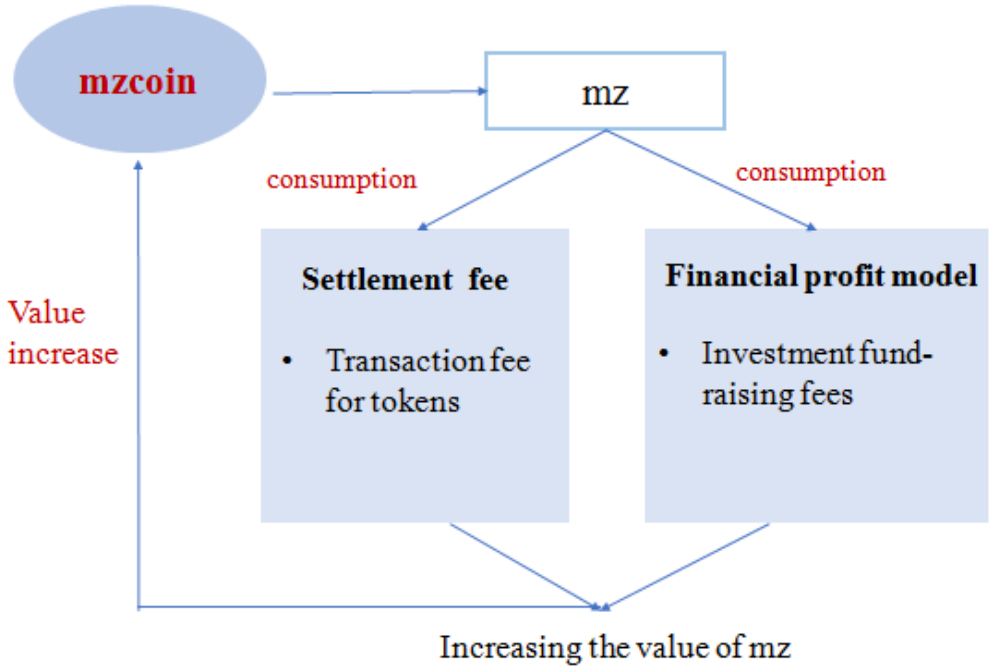


Figure 9-1 Mzcoin profit model

Chapter ten： Mzcoin council

10.1 Governing bodies

To ensure the openness and transparency of the mzcoin project, mzcoin is managed by the decision-making committee, the highest decision-making body. The decision-making committee shall have a business committee, a technical committee, an integrated services development committee, administrative organization will be composed of developers and functional commissions. Policymaking committee members are elected for a term of two years, the first decision committee members by mzcoin core team members, blockchain industry celebrities, legal experts and early investors, subsequent decisions members of committee will be elected by the community.

10.2 Director of the regulation

The mzcoin council is trying to establish a good governance structure and form a new type of coinage in the form of an association.

Intermediary agencies, implementing voluntary supervision and mutual trust between the two parties to help and manage the general affairs of the ecological community.

And privileges. The design goal of the governance structure of mzcoin council is to promote the community e-commerce self-drive association.

The sustainability of the project, the effectiveness of management, and the security of fundraising.

The ecological community governance of this project is mainly planned by the council. The legal guarantee will be known by our cooperation.

The name of the law firm, they will be involved in the entire mzcoin and its ecological community construction and development process.

To conduct legal advice and guidance on compliance with the law.

10.3 Governing team

10.3.1 Founding team.

1. **Tom Blomfield, CEO.**

Tom was founded GoCardless fintech, at the beginning of establishment,he raised $25 million, 2013, he was nominated as the European commission under the age of 30, one of the top five entrepreneurs, he often talks about the future of the Banks and fintech.

2. Paul ripon

Paul rippon, vice President and co-founder.

Paul has 23 years of experience in retail banking, with millions of clients in lloyds, the Irish bank Natwest. He lectures at the bank of London and the school of finance.

3. Tom

Tom was founded GoCardless fintech, at the beginning of establishment,he raised $25 million, 2013, he was nominated as the European commission under the age of 30, one of the top five entrepreneurs, he often talks about the future of the Banks and fintech.

10.3.2 Technical team.

1. **Bartek Nowotarski**

Bartek is a software engineer who focuses on the security of Internet applications. He received his bachelor's degree in computer science from Jagiellonia University. Before joining mzcoin, he worked at the development and security consulting association, and he found technical flaws in Facebook and Yahoo and proposed improvements.

2.Stefan Thomas

Stefan graduated from Russia with a master's degree in college physics from the university of fine mechanics and optical technology in Petersburg. He is a computer science expert and professional in statistics. Rich experience in advanced data science, applied mathematics, statistics and machine learning. With unremitting efforts, he has developed the most advanced innovative technology in neural network research. He has studied the unique data science method and brought a new perspective with the boundless enthusiasm of the blockchain technology and the great change of the Internet of things.

2. Christina Garman

Christina is a graduate of Stanford University in the United States. She has worked insamsung electronics co., LTD., 12 years' experience in software and Internet. She was a member of the research team at the business school software science institute. Her research interests included business process collaboration, workflow management, e-commerce transactions, service-oriented computing, software architecture, and software engineering. She joined the company in blockchain technology to provide

the white paper. She also served as an adviser to several blockchain technology start-up companies.

4.Nicolas Barry

Front-end technical expert, proficient in Node and IOS, familiar with most forefront front-end technology and server-side technology, familiar with the development of blockchain, and good at the implementation of application layer.

5.Holger Schinzel

Blockchain development engineer, familiar with all kinds of front-end technologies, with the front-end development capability across terminals and experience in designing and developing data visualization products, proficient in PHP, Node and Python.

Chapter 11: mzcoin release plan

11.1 Volume of issuance

Name of token: mzcoin.

Scrip: mz.

Total volume: 100 million issued.

Receiving currency: ETH. Mz tokens are based on ERC20 technology issued to centralize blockchain digital assets.

Crowd funding price: 0.16mz=1 yuan.

11.2 Release plan.

The total number of mz issues is 100 million, 40% subscribed by the founding team and the development team, and the number of subscriptions is 0.4 billion. 20% contracted by institutions, and the number of contracts is 0.02 billion. 10 per cent of issued by the market and the number is 0.1 billion; 10% private placement,0.1 billion; The number of crowd funding issues was 20 million.

The specific distribution plan is shown in table 11-1:

Table 11-1 MZ distribution plan.

比例 **Proportion**	数量 **Volume**	分配方案 **Distributed plan**
40%	40 million	Founding team subscription
20%	20 million	Institution subscription
10%	10 million	ICO public offering
10%	10 million	Private offering
20%	20 million	crowd-funding

11.3 Fund use plan.

40% of the funds are spent on technology research, finishing construction of the

mzcoin platform the main use channels are recruitment and supplementary research team, team incentive, etc.

15% of the fund will be used for promotion after the launch of mzcoin platform, including advertising, channel fees, etc. The online and offline combination of customers, the Internet and the traditional way of parallel.

15% of the fund is used for the promotion and distribution of mz currency, including the consulting fees required by mz and the promotion cost of the mz listed trading platform. In order to ensure mz can be launched on multiple platforms, we need to use some of the funds to launch other platforms, for the acceptance, use and transaction of mz can have a large space.

Thirty percent of the money is spent on peacetime security reserves.

11.4 The application of tokens

(1) Deductible service fee.

Mz tokens can be used to deduct the transaction fees generated by the transaction of the platform and deduct 0.35 yuan per mz. Mz tokens used for deducting fees will be destroyed directly and can be checked through the block chain browser to ensure transparency.

(2) Repurchase mz tokens.

The platform will use 50% of the quarterly net profit of the platform to Repurchasethe mz tokens. Supported by platform income, we will use 50% of the quarterly net profit of the platform in each quarter to repurchase, and the repurchased currency will be destroyed directly. Until the buyback destruction to the total quantity is greater than or equal to 100 million, the number of destroyed or repurchase to 8 times, through browser query blockchain, to ensure transparency, platform will hire external auditor to audit, every six months to ensure we offer 50% net profit to the mz tokens to buy back.