

# Calorie Chain

Provide professional customizable block chain solutions for corporate governments

Making blockchain business applications truly secure and private

## Catalogue

<b>Chapter 1 Summary .....</b>	<b>4</b>
<b>Chapter 2 Introduction to calorie .....</b>	<b>8</b>
2.1 Decentralization technology and privacy issues .....	8
2.2 Limitations of blockchain payment methods.....	10
2.3 Overview of the calendar chain framework .....	12
<b>Chapter 3 Design scheme .....</b>	<b>13</b>
3.1 Design principle .....	13
3.2 Implementation plan .....	14
3.3 Planetary chain safety protection measures .....	16
3.4 Smart contract 3.0.....	19
3.5 Getting out of chain data sources .....	21
3.6 Use of virtual machines .....	23
<b>Chapter 4 Solution example .....</b>	<b>24</b>
4.1 Supply chain .....	24
4.2 Internal special planetary chain .....	25
4.3 Game area .....	25
4.4 Education Department online classroom copyright .....	26
<b>Chapter 5 conomic model of incentives .....</b>	<b>28</b>
5.1 summary of current situation .....	28
5.2 economic network structure of calorie .....	28
5.3 economic design of calorie .....	29
<b>Chapter 6 Road Map .....</b>	<b>30</b>
6.1 Socrates .....	30
6.2 Platon .....	31
6.3 Aristotle .....	32
<b>Chapter 7 Team .....</b>	<b>35</b>
<b>Chapter8 Instructions .....</b>	<b>36</b>

---

8.1 risk reminders .....	36
8.2 disclaimer .....	37

# Chapter 1

## Summary

Blockchain technology has become more and more popular in recent years. It provides a new and efficient cooperation mechanism for human beings with a "decentralized trust" mechanism. The application of blockchain in the financial and commercial fields has brought the most attention and expectation. At present, all kinds of digital currencies have the basic functions of value transmission and value distribution, but they are far from the full-featured financial services needed in the real world, which is why the application of blockchain in the financial and commercial fields only hears thunder and doesn't see rain. In order to realize the blockchain value Internet era as soon as possible, people need a new generation of infrastructure based on blockchain technology, which has complete financial and commercial functions, can connect different communities and tokens, and can bridge the gap between centralized and decentralized organizations. Integration is inclusive. It should integrate the cryptocurrencies that exist and will be launched in the future, connect the centralized and decentralized organizations, accommodate the authentication mechanism and anonymous transaction mechanism, and introduce the data on and off the chain.

If you take a quick look around your office or home, most of the things around you come in some form, through different regions, countries or even global supply chains. But you may not know how these products flow to you. Not only you, but also the enterprises and manufacturers that produce these goods are facing the problem of improving the transparency of the supply chain. The root of these problems lies in the limited ability of sharing data in the whole supply chain.

A few years ago, some enterprises adopted such a solution: paste the exclusive QR code on the parts from all over the country or even the world. When these parts arrive at the destination and are ready for assembly, they can trace the source and logistics information of each part by scanning the QR code. This solution, to a certain extent, improves the transparency of information in the supply chain. But at the same time, this kind of solution also makes the production environment face the crisis of trust. Because

all of this can be fake. The QR code can be fake, the source can be fake, and the logistics information can also be fake, so this solution is not desirable in practice.

In addition to the issue of supply chain transparency, according to payoneer's 2019 global payment report, cross-border payment flow in 2019 was US \$209 trillion. Such a large payment flow has resulted in high transaction and remittance costs, which are increasing every year and are expected to reach US \$300 trillion in 2025. For smaller transactions, usually small and medium-sized enterprises, the impact is greater. In September 2018, the financial operation research institute's survey on the prospect of cross-border payment clearly pointed out that the high cost of cross-border payment transactions reduced the profit margin. The existing financial payment system can not fully meet the growing demand for payment, which leads to the huge loss of Global trade and economic development opportunities. It is necessary to innovate the financial payment mechanism to supplement the traditional finance.

Blockchain technology provides a way to build a public and distributed database or transaction group. These records or transactions are essentially encrypted, secure and irreversible. They use distributed consensus mechanism between nodes of the network to make or verify any changes to the recorded blockchain, so as to ensure that the nodes in the network are synchronous and always keep the latest state of the blockchain. The distributed decentralized feature of blockchain network and its consensus mechanism ensure that there is no central failure point in the system. It can be seen that there is a close relationship between the evolution of Finance and blockchain technology.

But at the same time, there is a new contradiction. When enterprises and governments want to choose a blockchain technology to solve their own problems, they usually encounter the following problems: which one should be chosen in the complicated public chain in the current market? In the complicated digital currency, which payment method should be chosen?

Indeed, all kinds of public chains are contending and all kinds of digital currencies are blooming. The emergence of blockchain technology itself is to solve the trust crisis. However, in the current situation of mixed market of blockchain technology, as an enterprise and a government, which chain and which currency should be selected, this has already brought a trust crisis. Because the security and stability of a public chain directly determine the security and stability of enterprise and government data. At the

same time, the smoothness of a digital currency in payment directly determines the security of assets of enterprises and governments in financial payment. So choice is crucial.

In 2014, Ethereum put forward the concept of ERC20 token, which makes it convenient to issue tokens. Government enterprises and individuals want to have exclusive tokens, which is no longer an insurmountable technology gap. To a certain extent, the ERC20 token of Ethereum solves the problem that government enterprises and various institutions choose a certain digital currency as their own market circulation means. Because they can issue their own tokens and use them as a means of circulation and payment. They don't need to choose from hundreds of digital currencies on the market, and they don't need to worry about their own choice of digital currencies. In the future, they may have various unpredictable problems. With the emergence of the concept of token, the government enterprises and institutions that choose blockchain technology as a solution can greatly improve their control over the means of circulation.

But at the same time, the solution faces a problem. Although the control of token is in one's own hands, the token is issued based on the third-party public chain. In the final analysis, it is still someone else's technology. When using someone else's bottom technology, it will still face a trust crisis.

In the blink of an eye, in 2020, today's blockchain development is more rapid, and people's recognition of blockchain technology is even higher. When the enterprise government and various institutions intend to use the blockchain technology to solve their own problems, they want to further improve the control of this technology, closer to the bottom.

At this time, we have a new solution called "planetary chain".

Planetary chain, also known as parallel chain. In the past blockchain and public chain technology, only users are allowed to issue their own tokens based on the public chain, and tokens only have circulation function. The transfer operation of token is completely handled and controlled by the company chain, and the user does not have any other permissions. In the Calorie chain, users can build and create their own "planetary chain" on the network. The "planetary chain" is independent of each other and has its exclusive consensus right. At this point, the Calorie chain can be compared to the "Star" in the network. "Planets" have their own specific orbits and do not interfere with each other.

Before the calendar chain, if we call the past era "the era of currency issue". Now, the era of chain is coming.

# Chapter 2

## Introduction to calorie

### 2.1 Decentralization technology and privacy issues

With the globalization of trade and the increasing complexity of supply chain, the degree of information asymmetry is further intensified, which makes the distribution of information among the stakeholders involved in the supply chain uneven. When the stakeholders come from different companies, there is no unified incentive policy to provide complete information, which makes the information asymmetry more acute.

Therefore, the final buyer of the product does not have a proper way to verify the product they purchased, which creates conditions for fraud. For example, counterfeit goods are rampant in the market, safety problems, violation of labor standards and so on.

Supply chain not only refers to the supply of means of production, but also includes the supply of information and data on the Internet. For example, Facebook lost tens of billions of dollars in market value in just two days due to the massive privacy leak in March 2018.

The reason why the Internet causes information leakage is that all data of users are stored in the centralized servers of companies providing websites or apps. And the company's own servers store and process information. The birth of blockchain network aims to establish a decentralized platform to store and process information to protect the privacy of users. However, in blockchain networks such as bitcoin or Ethereum, which have very low customizability, when the enterprise government and institutions use these networks, they can't completely customize functions according to their own needs, which will cause user privacy leakage.

For example, if you use a blockchain network with low customizability, such as bitcoin or Ethereum, to solve the payment problem, perhaps every offline purchase record and online purchase record of you will be published directly on the block browser. Anyone can see that everyone can find out how much money you spent on what items



at what time. In a way, this is a behavior of disclosing user information.

In fact, the digital assets and their transaction records in the blockchain network belong to relatively private and sensitive information. If they are transparent to all people and cannot be deleted, imagine that when the blockchain is implemented in a large number of applications in life, for the vast majority of ordinary life scenario needs, their transaction and payment information will be made public, which is nothing Doubt is unacceptable.

Therefore, we can draw such a conclusion. We only have specific requirements, need to use blockchain technology to solve, and need to achieve transparency and non tamperability. At the same time, there are also some scenarios where we do not want to make information transparent, such as the following situations.

- \* A company does not want its competitors to know its supply chain information;
- \* Some rich people do not want to be informed of their specific wealth by the outside world;
- \* Fund companies, securities companies, etc., do not want to be seen by other people's specific trading records, so as to prevent others from predicting their trading intentions, affecting trading and profits.

In the traditional blockchain network, all the information is transparent and cannot be deleted, which is obviously contrary to the actual application scenarios of enterprises, governments and various institutions, which hinders the further development of the application of blockchain technology.

Therefore, they need a common network which can be set with high system, pluggable modules and built on demand. Calorie chain is such a network.

The calorie chain is a highly modularized public chain bottom layer, which is also a very suitable development framework for customization. The "planetary chain" has strong scalability and supports the deployment of its own consensus and application ecology. Any enterprise, government and institution can be built on demand in the calorie chain, with a high degree of autonomy and control. The main chain, also known as "star chain", is only responsible for the operation of core functions to ensure safety, while complex functions are developed and operated on the "planetary chain", which are independent and complementary to each other.

## 2.2 Limitations of blockchain payment methods

On a global scale, the main reasons for the low efficiency of trade and financing development are the internal system of different enterprises is not connected, sometimes it needs to be handled manually, there are multiple intermediaries, and the trust environment between the parties.

If the enterprise government wants to use digital currency as a means of payment, although it can solve the above problems to some extent, it will also introduce other problems. For example, there are many kinds of digital currencies, and most of them cannot be transferred across the chain. Another example: the price of digital currency fluctuates greatly, if the transaction time is long, it is easy to generate disputes on the amount and so on.

In order to solve the above limitations, Calorie chain has improved from three aspects: interoperability, scalability and availability. The first is interoperability. Different blockchains, central organizations and data centers have different definitions of the value of something. If we want to achieve value unification, we need the public chain to be able to communicate different blockchains, different centralized organizations, different data sources, and not only be able to deliver value, but also be able to run other smart contracts. The second is scalability, which needs to be able to be used in different scenarios, including finance, manufacturing, government management, etc. Finally, the usability requires a resource rich ecosystem, a variety of dapps to run smoothly, developers to develop applications efficiently, and users to use applications easily.

\* Calorie chain cross chain atomic trading.

The value network not only needs cross chain communication, but also needs to communicate with existing centralized institutions and external data sources. Currently, the blockchain cannot interoperate with other blockchains (synchronize blocks of other networks), and tokens on different blockchains cannot trade with each other. At present, the blockchain cannot interoperate with the external centralized mechanism, which makes it difficult for the assets outside the chain to map to the chain. Because the current blockchain is unable to read the data outside the chain, it is difficult for the "smart" contract of the

current blockchain to be applied. Taking cross chain technology as an example, cross chain transaction is very difficult at present, let alone the development of cross chain smart contract. At present, there are thousands of tokens, but each token can only move freely on a single blockchain, and can only form its own wallet, its own smart contract and other ecosystems. The existing blockchain ecosystems are actually island ecosystems, far from realizing real interoperability.

Atomic trading technology provides a solution to this phenomenon. The specific implementation technology will be detailed in the next chapter.

#### \* Enhancement of smart contracts

As for scalability, it is still very difficult to map many scenes of out of chain actions to the blockchain. Previously, ICO projects can be carried out on the public chain through ERC20 and other agreements. However, financial, physical assets and various derivatives invested are still difficult to map to the blockchain. And in many off chain trading scenarios, as long as heavy calculation is involved, the demand for off chain data still cannot be mapped to the blockchain. Many projects are making relevant efforts, but this process is seriously hindered due to the lack of efficient cross chain communication solutions.

To this end, Calorie chain enhances the smart contract on the main network, realizes the application of multi-party digital assets, and has a variety of triggering mechanisms to effectively obtain the input of data out of the chain, and calls a variety of other smart contracts in a nested or parallel way, which improves the scalability.

#### \* Module pluggability

According to the previous chapters, in order to make blockchain technology truly applied in real life, blockchain network must have a high degree of customization, and must carry out specific analysis and development according to specific application scenarios. In the Calorie chain network, the main network is divided into six modules: wallet, P2P, block, store, MemPool and RPC. Developers can select and combine on demand to achieve their own actual needs, greatly improving the availability of blockchain technology in real

life.

## 2.3 Overview of the calendar chain framework

The calorie chain was developed using golang.

The architecture is shown in the figure below

Application layer
Incentive layer
Consensus layer
Network layer
Data layer

# Chapter 3

## Design scheme

### 3.1 Design principles

From the above analysis, we can see that the rise of blockchain enables people to see the future of the Internet. To a certain extent, blockchain represents the future of the Internet. However, the Internet still has bottlenecks in interoperability, scalability, availability and other aspects, which makes the current blockchain network difficult to support cross chain value transfer, cross chain smart contracts or cross chain applications.

As the blockchain network assets are presented in the form of tokens, as long as the multi token smart contract can be realized, the interoperability of the blockchain network can be greatly enhanced, and the scalability becomes easier. The current cross chain technology is generally the side chain technology, which moves the transaction to the side chain through two-way packaging, and then realizes the exit from the side chain through multiple signatures. Such a way can only achieve the same network transfer, and the performance is general.

If the "planetary chain" (parallel chain) solution is adopted, the core functions will only run on the "star chain" (main chain), while the complex functions such as virtual machine and smart contract will be solved on the "planetary chain", which can not only reduce the data processing capacity, but also have a complete blockchain ecosystem.

The economic activities on the blockchain network have just begun. In recent years, cryptocurrency has begun to penetrate into all aspects of life and grow rapidly, but its total value is only a few hundred billion dollars, compared with the existing global financial scale, it is a drop in the bucket. The total market value of the global land and real estate market, stock market, commodity market, foreign exchange market, bond market and derivatives market can be tens of trillion, tens of trillion, or even tens of billions.

Planetary chain technology can greatly reduce the cost of data link. Once a complete blockchain ecosystem is formed, the data on the chain will be more diverse. Just design the circulating token on the parallel chain, and more data can be mapped to the blockchain network. A large number of valuable things, such as land, houses, works of art, intellectual labor and other valuable things, are still not well displayed in the chain. With the continuous development of parallel chain and "token technology", asset token will become a new industry, and more and more value will flow in the chain.

## 3.2 Implementation plan

Taking cross chain technology as an example, cross chain interoperability is very difficult at present, let alone the development of cross chain smart contracts. At present, there are thousands of token and coin, but each token can only transfer freely in a single public chain, forming its own wallet, smart contract development tools and other ecosystems.

The existing blockchain ecosystem is actually an island ecosystem, and the value of blockchain network is far from real interoperability.

ross chain atomic transaction (taking cross BTC network as an example)

### (1) Start lock request

User a initiates 10 BTC lock requests to calorie by using the lock interface in the wallet.

### (2) Start private key

The lock request operation triggers the start of the lock smart contract and the initialization of the private key. The so-called private key is to generate a private key in a distributed way. In this process, the smart contract will complete the distributed storage of key fragmentation and key fragmentation. The initialization of the private key lays the foundation for the storage and use of the key.

### (3) Transfer the bookkeeping authority to the node management

After that, an address will be generated on the bitcoin network, and user a will transfer his BTC to this address. The user transfer operation will be initialized with a broadcast by the interface of the calendar, and the calendar node will check the completion of the transfer.

After receiving the transaction broadcast, the nodes on the planetary chain will check whether the transaction is confirmed on the bitcoin network through the interface. If the result shows that 10 BTCs have been successfully transferred to the address generated by the lock, the accounting authority will be transferred to the node management.

### (4) Map token

After confirming the transfer of bookkeeping right, the smart contract will update the account status of user a on the calendar. The locked record will be packaged by the node and recorded in the planetary block. At this time, 10 BTC lock requests to user a are completed.

Similarly, the user lock request is initiated in the wallet by calling the relevant program interface. The user experience with the wallet is similar to any token transfer. The specific steps of locking implementation process are as follows:

#### (1) Start lock request

User a operates the wallet to initiate a 10btc transfer transaction to a bitcoin address other than the calendar, which will be considered as a lock request.

#### (2) Check, lock, generate transactions

The transaction triggers a locked in smart contract on the calorie. The contract will first check the asset status of user a on the calendar, lock the status of 10 bitcoins mapped by user a in the calendar account, and then generate a transaction request signed by user a for addressing.

#### (3) Node signature

The nodes in the planetary chain receive the transaction request and start to calculate and compare according to the key fragments stored in them. If the result is



positive, the node will sign and broadcast the result.

At the same time, each node collects signatures. When the transaction signature reaches 3, the transaction is sent from the node to the bitcoin network, and the transfer of 10btc transaction is completed.

#### (4) Decompose node control

The nodes on the calendar will check whether the transaction is confirmed on the bitcoin blockchain through the bitcoin corresponding interface. After the transaction consensus is reached and confirmed, user 10btc will disassemble the node control.

#### (5) Release token map and destroy

The smart contract will synchronize the user's status on the calorie account, release the locked 10 BTC mappings, and destroy the mappings. At the same time, locked records are packed into planetary blocks. At this point, the user's lock request is complete.

Nodes participating in cross chain transaction initiation, transaction confirmation and transaction signature verification will receive corresponding rewards according to the given incentive mechanism.

### 3.3 Safety protection measures of planetary chain

#### Account system

The use of private key of account system is realized by distributed password calculation. When a transaction signature verification is broadcast, the node can calculate and compare it according to its saved fragments. When the verification is successful, the nodes sign and broadcast the verification results of their fragments.

At present, the calorie team has come to the conclusion through code analysis that hash 256 and elliptic curve algorithm can support private key sharding and distributed



computing. For some original chains, if the algorithm doesn't support fragment computing, homomorphic encryption will be considered to realize the key computing without disclosing the key.

### Consensus system

The security of the consensus algorithm depends on the randomness of the nodes that generate each block. When the malicious nodes can't get the generation right of continuous blocks by controlling the computing power, the security of consensus algorithm can be guaranteed.

The randomness design of the bookkeeping right is similar to "lottery". That is to say, through a certain algorithm, a large number of randomness of "lottery" is given to the process of "winning" node to ensure that the results of each node are unpredictable. This consensus mechanism is known as "PoS".

The following is the method used to select the accounting node:

First of all, if you want to be a node with bookkeeping rights, the node account must contain the calorie coin. Nodes participating in bookkeeping are generated based on POS consensus algorithm. Nodes with more currency and longer currency holding time are more likely to become bookkeeping nodes.

Then the nodes are grouped, and the results are generated by calculating the hash value of the previous block and another input value, and then grouped by a preset function. The grouping process is a random process, which has nothing to do with the amount of money and the age of money.

Finally, the packing nodes are selected according to the calculation force. The POS mechanism encourages bookkeeping competitors to have some computing power, but does not encourage them to have too much computing power. At the same time, the mechanism guarantees the randomness of the generation of the packed nodes. Of course, there will be more opportunities for nodes that master the highest computing power of the network, but it is still difficult to ensure frequent "winning" because of randomness.

To sum up, although a node spends a certain cost to maintain its equity or increase

its equity in order to achieve more bookkeeping opportunities, it does not guarantee that its "winning" opportunity remains at a fixed value. At the same time, by adjusting the number of groups, through our randomization and distribution mechanism, we still have enough opportunities to obtain accounting rights for nodes that do not hold a large number of interests or have absolute computing power advantages. In this way, more nodes are often treated more rationally. In the end, most nodes are in average state. Moreover, with the increase of the number of network nodes, this balance will not change significantly.

Therefore, the calorie chain will always maintain a high degree of randomness.

The high degree of randomness can also be reflected in the grouping of the second step. Suppose that the nodes in group A want to get the packaging right of group B transactions. First of all, it will face the competition with group B node, and can not guarantee that the node will win in the competition. And even if the node succeeds in becoming the winning node of group B, before group B transactions are submitted to group A, they will be submitted to a specific smart contract, which will be kicked out and discarded by the contract.

Therefore, in this case, node A makes a useless effort. Similarly, a malicious node cannot be controlled in this way.

Make two consecutive blocks to perform a malicious fork.

At the same time, Calorie further increases the randomness. A specific smart contract can set a group of  $N$  groups as a walk node, and divide all transactions into  $N+1$  groups. The so-called walk node is that these nodes are given the right to choose any group to join.

Assuming that the nodes in the whole network are honest nodes, the existence of wandering nodes will inevitably further increase the randomness of the accounting rights of nodes, resulting in greater uncertainty of the results.

These uncertainties increase the cost for malicious nodes to obtain the packaging right by attacking the node, and even if

There is no guarantee that the package right of the previous block can be obtained. It is very difficult to attack and control too many nodes, because the number of nodes

is at least equal to the number of groups, and this is already a very large number, which will attract the attention of the whole monitoring system.

### Hierarchical system

The layered system is embodied in the work of packing blocks. It divides it into two stages, corresponding to two levels of processing.

The first layer is the application execution layer, which records the execution results of the application and submits them to the second layer. The second layer is the block generation layer, which packs the results submitted by the first layer to form the block record on the chain.

In the first layer, the application computing layer, the planetary node completes the processing of all current transactions to achieve the parallel computing of all current transactions. In addition, the processing power of things is packed by randomly selected nodes in each round, which increases the security and scalability of the algorithm.

## **3.4 Smart contract 3.0**

Asset tokenization is actually a process of transforming off chain value into digital assets and decentralizing, digitizing and programmability of these assets. The process of token and the whole transaction of token in blockchain network belong to the category of cryptofinance.

The most important feature of cryptofinance is that assets and value are mainly embodied in the blockchain, whose property right is mainly controlled by private key, and transaction activities are mainly completed by smart contracts on the blockchain.

Due to the advantages of smart contract, it will have an impact on the existing financial operation mode. Off chain assets will be tokenized into encrypted financial assets. Smart contracts can call "encrypted data (balance)" in different addresses. Therefore, smart contracts can nest with each other to express complex financial logic and form applications that traditional finance cannot achieve.

### **Cross chain smart contract call rules**

In the code of the smart contract in the calorie chain network, the pre-set condition judgment and pre-set condition rules for calling other public chain smart contracts are added, and the parameters of the address index of the target smart contract are created. The basis of condition judgment comes from the data input and the result of data calculation when the calorie smart contract is triggered. If the default conditions are met, the node will download other public chain smart contracts and execute them.

There are two parts to describe the calling condition: rule and timing. A rule is a computational function written in advance in a smart contract. The timing condition may be the default condition in the smart contract, or it may be the real-time condition for regularly checking the status of the smart contract.

### **Cross chain smart contract calling process**

Suppose that the smart contract in the calorie network is a, and the only contract in other public chains is B.

I. When smart contract a is triggered, it will judge whether smart contract B needs to be executed according to the preset call conditions.

II. When the call conditions are met, the preset calculation function is executed, and the calculated result will be the input of smart contract B.

III. nodes that have executed smart contract a download smart contract B locally, input the data calculated in the previous step as the data input by smart contract B, and start executing smart contract B.

The above steps can complete the call of smart contract a to contract B. because smart contract B is based on the state of smart contract a as the trigger and input data, we call the logical relationship between them as the connection call of smart contract.

The smart contract 3.0 proposed by calorie not only makes judgments according to its own logic, but also calls other smart contracts through preset conditions. In this way, we can build a network like call relationship between different smart contracts. It provides the possibility to build interconnected financial applications and other complex applications through the title between smart contracts

Then call to build complex financial and supply chain services.

## 3.5 Get out of chain data source

### Off chain data source interface call

Smart contract 3.0 can also use off chain data in triggering conditions. Generally, such data acquisition is conducted through standard HTTP or socks based API provided by a third party. For example, a third-party interface calls a function to get the address of the target URL through HTTP and get a JSON packet.

This interface method is also applicable to the use of calendar to obtain information on other blockchains, such as querying and confirming whether a transaction on another chain is confirmed by the block. It can also be used to transmit third-party data, such as stock index, football match results, weather data, etc.

Calorie smart contract 3.0 will use the basic data to identify the third-party interface and form the corresponding third-party interface for the smart contract to call.

In previous blockchain landing applications, the following core problems need to be solved:

How to ensure the authenticity and consistency of data? Which one shall prevail in

case of inconsistency? When it is necessary to read data, is it on or off the chain? What data is linked and what data is not linked?

According to the above problems, in the calendar network, both ends hash the data once, which can quickly compare whether the data is consistent. At the same time, the front-end is through the chain and the back-end is through the database. The front-end is to provide services for users, so the data on the chain should be taken, and the back-end is managed. You can directly take the database, and then ensure that the database and the blockchain data are consistent.

Finally, sharing data is linked, private data is not linked. In the parallel chain system, when it is necessary to share data with other members, the API interface can only be used before. With the blockchain technology, the problem of resource sharing can be solved better.

To record multimedia data, such as pictures, audio and video, it can be integrated into the collection terminal, and then uploaded to the decentralized distributed file system asynchronously. The decentralized distributed file system can realize that each image or audio corresponds to a unique hash value, then the image can be accessed through the hash value, and the image is synchronized to the adjacent nodes to realize decentralization. If the image is modified, the hash value will change and the data will be invalid.

## **Multiple trigger recognition**

The existing smart contract can only wait passively for the trigger of the transaction and can only be executed by the transaction on the chain. The key words recognition trigger function of the information outside the chain is added to the calendar, and the related smart contracts will be automatically run by multiple triggers, so that the smart contracts can be activated in succession without the need of human. Therefore, multiple parties can trust each other through the smart contract code to complete various complex financial functions. Taking borrowing money to participate in the application of ICO as an example, the calorie smart contract can be programmed to borrow tokens, return new currency and pay interest. Taking the fund application as an example, the smart contract on the calendar platform can automatically manage a fund, invest various tokens in various digital assets, generate management fees, pay dividends, etc., at the same time, it can accept margin, and realize the functions of adjusting margin, clearing and settlement through triggers of external data sources.

## 3.6 Use of virtual machines

In terms of programming language, Calorie uses Go language, and developers can use Go language to quickly migrate existing smart contracts.

In the future, we will provide compilers in different languages to support more smart contracts.

In terms of virtual machines, because Solidity is currently the most commonly used language for developing smart contracts, Calorie initially used EVM for compatibility.

In the long run, we will use more development resources in the JVM. At the same time, for developers who are unable to use blockchain virtual machine skillfully for the time being, we also provide encapsulated interfaces of Java, PHP, Python and other common languages for developers to call in the early stage, so as to get started faster. In this way, more and more developers are attracted to join the open source community of Calorie to jointly create an application ecosystem and promote more high-quality DAPP applications.



# Chapter 4

## Solution examples

### 4.1 Supply chain

Logistics enterprises are facing an unprecedented era of change, digital is occupying a leading position, and customers' expectations are also rising. Blockchain technology is realizing higher efficiency and more convenient cooperation mode, ensuring authenticity at delivery, transparency and providing instant settlement.

With the use of calorie chain, the participants in the supply chain can cooperate with each other by using smart contracts that are developed in advance according to payment terms. The Internet of things and other real-time monitoring technologies can be used to track delivery and update access status in real time. After successful delivery, smart contract can issue payment to all supply chain participants at the same time according to the agreed payment terms. With blockchain, all parties can ensure the transparency of delivery and payment. Transportation costs can be minimized by timely payment to logistics providers through transparent smart contracts. The rating system can further improve the practicability of smart contract solutions and track the real performance of supply chain participants over a period of time.

In addition, all employee records can be kept in designated ledgers between the company, bank and selected suppliers. Using the block browser, transactions can be viewed in real time at any time, eliminating the need to obtain daily reports of services provided from suppliers. When the employee's request matches the identification field in the supplier's response, the transaction is approved and uploaded to the blockchain, eliminating the need for manual reconciliation. This safe and simplified process minimizes the cost of human intervention and processing and can save customers a lot of money.



## 4.2 Internal special planetary chain

One of the disadvantages of public blockchain and public chain is the absolute openness of information, which means that the privacy of transactions is very poor. Most of the time, enterprises and government departments only need to make the transaction data absolutely transparent to the inside and keep it absolutely confidential to the outside.

Another disadvantage of public blockchain and public chain is that they need a lot of computing power to achieve consensus. These factors make them unsuitable for commercial and political use, especially for use cases involving payment and settlement.

The planet chain of calorie is highly customizable. Enterprises and governments can create private networks through the planet chain. By creating a private private network, the internal personnel can be connected safely and privately, and the transactions under the private network can not be seen by the outside world, so that the sensitive financial information and transaction information are absolutely safe and confidential. For example, banking organizations can use

Blockchain technology simplifies reconciliation process and business process, including payment service, financing loan portfolio, asset financing, equity and other derivatives and other complex products. A planetary chain can be shared within the bank, which only allows internal personnel to read and account. Although data and state changes are recorded on the blockchain network, any transactions between internal personnel are invisible to the outside world.

## 4.3 Game area

The field of online games is one of the most open and transparent fields. Many people who know about the game have played "private server", that is, the server set up by private. In the private server, the administrator can modify the attributes and money of the characters in the game, or the attributes of the monsters, with highly centralized power.

Also, even if it's not playing games in a private server, it's on an official server. This phenomenon of "dark change" is also common.

For example, there may be internal staff in the server, commonly known as "trust".

Managers can secretly modify their money balance in the game to achieve the effect of stimulating real players to recharge. For example, the game administrator, in order to achieve a certain purpose, will often secretly modify the difficulty of the game, such as increasing the monster's attack, blood volume and so on.

All in all, the high concentration of power in the game field is very unfair to the players.

However, in the field of games, it is also very suitable to use blockchain technology to solve pain points, such as character attributes, package amount, monster value and other contents, which are very suitable for going on the chain to ensure the transparency and openness of data and improve the fairness for all game players.

Today, the parallel chain of Calorie can better apply the blockchain technology in the field of games. By creating multiple parallel chains with different division of labor, you can immediately chain up dropped equipment, upgrade people, change people's status, pass levels, etc.. This will completely guarantee the fairness of all players, no centralized administrator can change the data secretly, and there is no possibility of malicious attack on the central server by players To tamper with data.

## 4.4 Online classroom copyright of Education Department

Online classroom and online education are a trend. According to YouTube statistics in 2018, 73% of primary and secondary school students have used online education to listen to online courses, with an average of more than 50 hours per month to watch online courses, and an average of more than 200 dollars per year spent on online courses. Online education platform is the coming turyere, which is about to usher in the breakout point.

But the corresponding problem is the copyright of online courses. Piracy is very serious. A set of online courses has been transferred to another level

Layer upload to different online platforms many times, it is difficult to trace back to the original author. And the same set of online courses, the price gap between different platforms is large. This makes the education department unable to regulate and manage the online course market efficiently, and misses the way to broaden the learning channels of local students. The online teaching resources are seriously inconsistent with the needs of users.

And the planet chain solution of calorie can build a planet chain for each online course platform designated by local students. Each original online class video will have a unique hash value corresponding to it. When the video is uploaded to a planetary chain for the first time, the hash value will be recorded by the star chain, and the uploader will get a certain number of tokens as incentives. When the same video is uploaded multiple times, and the star chain detects the duplicate hash value, it will reject the request to upload the video to the planetary chain through the smart contract. At the same time, students also buy online courses by paying tokens, which are transferred into the blockchain wallet of the original author of online courses according to a certain reward share in real time. The proportion share is written into the smart contract, which can't be modified by anyone. It also fundamentally prevents the platform from withholding or delaying wages, so as to encourage more online course creators to upload more high-quality online courses.

# Chapter 5

## Economic model of incentive

### 5.1 summary of current situation

If the vast majority of public chains on the market are compared to a business district, the first thing they do is to delimit the scope of their own business district. But after a period of time, there are no buildings, shopping malls or entertainment facilities on the land, which is very desolate.

The economic model of calorie is to build buildings, shopping malls and various entertainment facilities on the land first. When these facilities are built, the scope of the business district will naturally form, or even expand infinitely.

### 5.2 economic network structure of calorie

An ideal blockchain economic model should include public chain and coin and be composed of multiple levels. Using the concept of "planetary chain", calorie is committed to building a credible network. The network structure of calorie is mainly divided into three layers: trust layer (account layer), construction layer and contract layer. Each layer also has its corresponding economic model.

1. Trust layer: the trust layer is the ledger layer, which provides the most basic consensus services to the outside world. For example, each transaction of the planetary chain will be agreed twice, the first time in the main chain and the second time in the parallel chain itself. Therefore, the security of the planetary chain is guaranteed by its parallel chain and the main chain. During the first consensus, it will consume calorie as a withholding fee and fuel, which will increase the scarcity and demand of calorie.

2. Construction layer: the construction layer mainly includes virtual machine service and parallel chain building service. When the parallel chain is released, in order to prevent malicious branching in the future, a certain amount of calorie needs to be submitted as collateral.

3. Application layer: the application layer mainly includes all kinds of smart contracts and decentralized PAAS. At the same time, it can provide encapsulated transaction interfaces to accelerate the circulation and transaction frequency of calorie.

Through the above three-tier architecture, the calorie network provides a credible service platform and ecosystem for government and enterprise computing in reality.

### **5.3 economic design of calorie**

Coin Name: calorie

Consensus mechanism: PoS

Total issuance: 100 million

Block out time: 6S

Blockbuster reward: 6calorie

Block halved height: 9413191

From the perspective of the ecological construction of the calorie, because the platform provided by the blockchain is a fair value circulation platform, the cost of generating economic behavior on the platform is only the transaction cost, and when generating economic behavior on the calorie chain, it consumes the calorie. The 100% of the calorie coin is completely obtained by the miners. Everyone has equal opportunities to participate in the mining, and absolute fairness is guaranteed.

# Chapter VI

## Road Map

We use the most famous ancient philosopher as the code for the release of the edition. They have made great contributions to the world in their own fields with their dedicated spirit and persistent habits.

### 6.1 Socrates

This stage is the first stage of the calendar, mainly around the development of the underlying technology and public chain technology.

#### March 2019, test network release of calorie

- \* Complete the underlying structure of the main chain of the calorie
- \* Support block chain, consensus, logic executor, P2P, MemPool, state tree storage, list storage, RPC and other block chain underlying support modules
- \* Support the pluggable consensus protocol, so that the calorie is not only a public chain system, but also an alliance chain and a private chain
- \* It supports a variety of actuators, system customization and user expandability

#### 2019.5 official online release of calorie

- \* Support the integration of Ethereum EVM virtual machine into the calorie system, support multiple storage methods and pluggable database
- \* Support transaction privacy protection

### **September 2019 planetary chain test network release**

- \* Support the planetary chain technology, and support the cross chain of the main chain and the planetary chain, as well as the cross chain asset transaction between the planetary chain.
- \* Smart contract Commission

### **November 2019 official network release of planetary chain**

- \* Support the integration of wasm virtual machine into the planetary chain
- \* Basic framework for SaaS and Las

## **6.2 Plato**

This stage is the second stage of calorie, mainly focusing on ecological construction and community building.

### **Global node deployment**

- \* Core code GitHub open source
- \* Diggable wallet upload GitHub for users to download and deploy
- \* Preliminary formation of global ore pool scale

### **Open Source Toolkit Online**

- \* Support visual guided token release

- \* Support user led deployment of private chain and planetary chain
- \* Atomic Trading (decentralized flash exchange) function online
- \* Decentralized chat function online

### **Eco software online**

- \* Support the realization of SaaS platform and LAAS system of supply chain finance and build a complete ecological software of Supply Chain Finance
- \* Realize and tap the commercial value of calorie, with more than 10 commercial parallel chains
- \* Cooperate with multiple centralized organizations and data sources to write data from multiple off chain data providers into the chain, so that more and more value can run on the platform

### **Interface standardization**

- \* By launching the "blockchain interface standardization campaign", the bottleneck of interoperability in the calorie network is solved.
- \* Through the standardization of the interface, the cross chain interaction between the calorie and other public chains can be fully realized, and the call between the calorie smart contract and other blockchain network smart contracts can be realized, which greatly improves the availability and expansibility of the calorie in the actual application.

## **6.3 Aristotle**



This stage is the third stage of calorie, mainly focusing on the prospect of blockchain technology development in the future.

### **Parallel chain Property Right Registration Platform**

- \* The biggest advantage of calorie in using blockchain technology lies in the convenience and low cost of registering information in its parallel chain technology. Each kind of information and property rights that need to be registered can be registered and recorded in a parallel chain area. The type of property right in society has been seriously restricted by the existence of registration cost. If we can reduce the cost of registration to extremely low or even zero through the parallel chain technology of calorie, then many new types of property rights will appear and be registered on the chain. The continuous enrichment and expansion of the types of property rights will improve the further promotion of human's "intellectual" labor status, not only contribute to human society, but also may change the mode of economic operation.

### **Hybrid blockchain architecture**

- \* The calorie hybrid architecture is based on the example of the alliance blockchain, which is different from the traditional private / alliance blockchain and public blockchain. There are different types of components in the public state of the calorie hybrid network, which are shared by all participating nodes. A node group can further form a network with its own private state, which is only accessible to authorized members. Private network status in

They are maintained in their respective networks, but records (hashes) of transactions and smart contracts are stored in the public state of the blockchain. Public state can be used to share other data safely and transparently across the calorie network, while private state can be used to protect sensitive data

- \* Data and financial data are not subject to external interference. The hybrid architecture of calorie can completely solve the contradiction between the transparency of blockchain and the anonymity privatization.

# Chapter 7

## Team

Bernoulli Blockchain & Intelligence Lab.

The laboratory is a scientific research team composed of cutting-edge people from academia and industry. The laboratory was founded in 2015. Since its establishment, it has long been committed to the research and development of blockchain based security solutions and application systems. At the same time, it has served as the design work of many enterprise network computing and Internet of things. It has landed many blockchain application scenarios and accumulated rich experience in blockchain technology implementation.

Bernoulli blockchain intelligent laboratory successfully combined the intelligent parking system with the blockchain technology by using the blockchain open platform in 2018, and put the parking space data on the chain by the way of decentralization, ending the disadvantage that the data can only be stored and called through the third-party organization in the past. It ensures the authenticity of parking spaces and the accuracy of parking success, and makes parking data traceable.

At the same time, the laboratory takes into account the availability of academic scientific research and technology in the industry, and completes the realization of practical application on the basis of in-depth theoretical research. Driven by big data and blockchain technology, the laboratory has been exploring the reform and innovation of Finance and data technology for a long time.

# Chapter 8

## Notice

### 8.1 risk tips

Systematic risk: refers to the possible change of earnings due to the common factors of the whole situation, which affects the earnings of all securities in the same way. For example, policy risk, the current national regulatory policy for blockchain projects is not clear, there is a certain possibility of loss to participants due to policy reasons; in the market risk, if the overall value of the digital asset market is overestimated, then the investment risk will increase, and participants may expect the project growth to be too high, but these high expectations may not be achieved. At the same time, systematic risk also includes a series of force majeure factors, including but not limited to natural disasters, large-scale failures of computer networks in the global scope, political turmoil, etc.

Risk of lack of market supervision: digital asset transactions, including calorie, are highly uncertain. Due to the lack of strong supervision in the field of digital asset transactions, there is a risk of sharp rise and fall of electronic tokens, which are manipulated by dealers. If individual participants lack experience after entering the market, it may be difficult to resist the asset shock and psychological pressure brought by market instability. Although academic experts, official media and so on all give advice on prudent participation from time to time, there is no written regulatory method and provisions, so it is difficult to effectively avoid this risk at present.

Regulatory risk: there may be regulatory regulations in the future to regulate the blockchain and electronic token fields. If the regulatory body regulates the field, the purchased tokens may be affected, including but not limited to fluctuations or restrictions in price and ease of sale.

Inter team risk: Currently, there are many teams and projects in the blockchain technology field, with fierce competition, strong market competition and project operation pressure. Whether the calorie project can break through in many excellent

projects is widely recognized. It is not only linked with its own team ability, vision planning and other aspects, but also affected by many competitors and even oligarchs in the market. In the meantime, it is possible to face vicious competition.

Technical risks of the project: first, the project is built on the basis of cryptography algorithm, and the rapid development of cryptography is bound to bring potential risks of being cracked; second, technologies such as blockchain, distributed ledger, decentralization and tamperability support the development of core business, and the Tron team cannot fully guarantee the implementation of technology; third, In the process of project update and adjustment, it may be found that there are loopholes, which can be remedied by issuing patches, but the degree of impact caused by loopholes cannot be guaranteed.

Hacker attack and crime risk: in terms of security, the amount of a single supporter is very small, but the total number is large, which also puts forward high requirements for the security of the project. Electronic token has the characteristics of anonymity and hard to trace. It is easy to be used by criminals, or attacked by hackers, or may be involved in illegal asset transfer and other criminal acts.

Other risks unknown at present: with the continuous development of blockchain technology and the overall situation of the industry, Calorie may face some unexpected risks. Participants are invited to know the overall framework and ideas of the project, adjust their vision reasonably and participate rationally before making the decision of participation.

## 8.2 Disclaimer

This document is for the purpose of conveying information only. The content of this document is for reference only and does not constitute any investment and sale proposal in Calorie.

The content of this document should not be interpreted as forcing participation. Any action related to this white paper shall not be considered as participation, including the requirement to obtain a copy of this white paper or to share it with others.

Participation in the project represents that the participants have reached the age standard and have complete civil capacity.

The community will continue to make reasonable attempts to ensure that the information in this white paper is true and accurate. During the development process, the platform may be updated, including but not limited to the platform mechanism, token and its mechanism, token allocation. Some contents of the document may be adjusted in the new version of the white paper as the project progresses. Participants are required to obtain the latest version of the white paper in a timely manner and adjust their decisions according to the updated contents. The team will not be responsible for the loss of participants due to their reliance on the content of this document, the inaccuracy of the information in this document, and any actions caused by this document.

The team will spare no effort to achieve the goals mentioned in the document, however, due to the existence of force majeure, the team can not fully make the commitment to complete.

As the official token of calorie chain, calorie is an important tool for platform performance, not an investment product. As an encrypted token used in the calorie chain, calorie does not fall into the following categories: (a) currency of any kind; (b) securities; (c) equity interests in legal entities; (d) shares, bonds, notes, warrants, certificates or other instruments conferring any rights.

Whether or not the value-added of calorie depends on the market rules and the demand after the application is implemented. It may not have any value. The team will not make a commitment to its value-added and will not be responsible for the consequences caused by its value increase or decrease.

To the maximum extent permitted by applicable laws, the team shall not be liable for the damages and risks arising from participation in the project, including but not limited to direct or indirect personal damages, loss of commercial profits, loss of commercial information or any other economic losses.

The calorie platform clearly conveys the possible risks to the participants. Once the participants participate in the project, they have confirmed to understand and recognize the terms and conditions in the detailed rules, accept the potential risks of the platform, and bear the consequences.

# Calorie Chain