

HCM White Paper

The new retail platform based on blockchain technology

Chengdu Wumeng E-Commerce Co., Ltd

May , 2018

Directory

Introduction.....	1
Chapter 1 Project Background.....	2
一、 Market Background.....	2
二、 Problems.....	3
Chapter 2 Project Origin.....	4
一、 Solution Ideas.....	4
二、 Solutions.....	4
Chapter 3 Business Model.....	9
一、 Basic Mode.....	9
二、 User Value.....	10
三、 Application Scenario.....	10
四、 Future Development.....	12
Chapter 4 Technical Realization.....	14
一、 Technology Architecture.....	14
二、 Technical Features And Advantages.....	21
Chapter 5 Core Values And Differentiation Presentation.....	25
一、 Physical Asset Endorsement.....	25
二、 Financial Services.....	25
Chapter 6 Release notes.....	27
一、 HCM Digital Currency Introduction.....	27
二、 Issuance Plan.....	27
三、 Fundraising Use.....	28
Chapter 7 Governance structure.....	29

Chapter 8	Team Introduction.....	30
Chapter 9	Risk Warning and Disclaimer.....	33

Brief introduction

With the maturity of blockchain 1.0 represented by Bitcoin and blockchain 2.0 represented by Ethereum, the blockchain has been come out of the conceptual stage, and will then step into the blockchain 3.0 era. The blockchain 3.0 will break through the scope of cryptocurrency and financial applications, it will be combined with practical applications in various industries and allowing users to feel the real value of the blockchain.

In recent years, the retail industry is booming and the scale continues to expand , the industry has continued to innovate, online retail has developed rapidly , and offline stores have also actively followed up. But no matter of how hot the concept is, consumers are still concerned about the quality and price issues. In the new retail area, there are still many problems such as price discrimination, rampant fakes, loss of privacy and etc. Under the traditional centralized organization system, these problems are difficult to eradicate.

To solve these problems, our team developed the HCM project based on blockchain technology. Our project uses the decentralized characteristics of the blockchain and combines with new retail formats, intent to create a decentralized digital currency payment network. It can provide safe and convenient currency payment channels to the parties, it also can provide consumer protection for the transaction to the customer. We hope to further optimize the advantages of cryptocurrencies, such as fast trading, low cost, high efficiency and etc, allowing merchants to trade with cryptocurrency holders who from around the world.

【Mission】 : The development team will create a decentralized digital currency payment network to meet the needs of rapid payment in offline retail payment, online commerce, asset exchange and other area.

HCM adopts the DPOS consensus mechanism, distribute 1 billion digital currencies in a constant amount. It not only can be used in the new retail consume shopping field, but also can be used for investment and wealth management.

Chapter 1 Project Background

1、Market Background

【Consume payment】 : Since 2016, the National Development and Reform Commission, Ministry of Industry and Information Technology and other ministries have issued policies on promoting consumption in many times. At the end of April, 24 departments including the National Development and Reform Commission, the Ministry of Education, and the Ministry of Industry and Information Technology jointly issued the "Notice on Printing and Distributing Action Plan for Promoting Consumption-led Transformation and Upgrading" and issued the "Top Ten Extended Consume Actions". Many provinces, municipalities, and autonomous regions have issued policy documents to promote consumption including Jilin, Guangxi, Liaoning, Gansu, Zhejiang and etc.

According to statistics data of the National Bureau of Statistics, the national online retail sales amounted to RMB7175.1 billion, an increase of 32.2% over the previous year in 2017. Among them, the physical goods online retail sales was RMB5480.6 billion, an increase of 28.0%, the proportion of total retail sales of social consume goods is 15.0%. In the online retail sales of physical goods, food, clothing and commodities respectively grew by 28.6%, 20.3% and 30.8%.

The "Better Than Cash Alliance" of the UN agency, announced the report that "What does the development of social networks, e-commerce, and China's digital payment ecosystem mean for other countries?". The report shows that under the promotion of Alipay and WeChat payment, the market size of China's social network payment (Alipay and WeChat) reached USD 2.9 trillion in 2016, which has increased 20 times in the past four years. The report shows that the digital payment methods of existing platforms and networks have not only to made people enjoy more extensive digital financial services, but also expanded the financial inclusion and economic development opportunities of China and neighboring countries. The report also predicts that the proportion of mobile and Internet payment will increase to 28% in

China's consume payment method, while the cash payment ratio will drop to 30% by 2020.

【New retail market】 : In recent years, the development of online retail is very fast, and the growth rate of physical stores has been relatively slow, this is a clear contrast between the development of rapid and the development of slow. Therefore, some experts, entrepreneurs, and social professionals make the online and offline to confronted, they think that online retail creates a lot of pressure on physical stores, and even online retail will replace physical stores. However, from the situation of domestic and international research, and from the experience of developed countries, in the early days of online shopping development, there was indeed competition between online and offline. But with the continuous development of online shopping, the competition gradually turned into cooperation and integration. The integration and development of online and offline can complement each other and it is the future direction of development of the retail industry. At the Alibaba Computing Conference in October 2016, the Jack Ma put proposed a new retail sales for the first time in his speech. "There will be no e-commerce, only new retail , in the next ten or twenty years. " According to the "Analysis Report on China's Retail Industry Market Forward-looking and Investment Strategic Planning for 2017-2022" released by the Industry Research Institute of Forward-looking Industry: In 2017, the transaction volume of China's new retail stores will reach to RMB 38.94 billion, and it will reach to RMB 1.8 trillion by 2022, and the compound growth rate will reach to 115.27%.

2、 Problems

While domestic digital payment and the huge size of new retail market, but there are still many problems in the practical application , for example :

1. Exorbitant prices: Because the market is not transparent, it caused some sellers not to set prices according to reasonable profits, and make the price high increase. Gaining huge profits in the case of market information asymmetry, this has seriously

affected the normal order of the commodity retail market.

2. Shoddy: In the temptation of high prices, some unscrupulous merchants use the fake and shoddy goods to imitate the quality product and deceive consumers. Due to the lack of relevant knowledge, the ordinary consumers are often difficult to distinguish between genuine and fake. In addition, Some merchants also make huge profits through fictional vendors and confused commodity grades. It make the consumer's rights have been greatly damaged.

3. The lack of transparency mechanism: Most businesses want to maximize their own interests, they will try to hide for the user all kinds of information that should be told, and gaining profits from the information difference. For example, recently the everyone knows thing of Ctrip "Deceive an acquaintance" (The purchase price of old customers is more expensive than that of new customers). It is a kind of transparency mechanism that brings price discrimination to users.

4. The leakage of user privacy: The current e-commerce retail platform is a centralized structure. The user's data is stored on the site's server. Once the server encounters problems or is used maliciously, the user's information will be leaked. (This is a typical example than Facebook leaking the user information events recently)

As we can know from the above expound, under the existing technology environment, there are many problems in the new retail sector in terms of price, product quality, user factors and etc. If we can solve these problems in a one-stop way by advanced technology, it will inevitably open up a new and broad market.

Chapter 2 Project Origin

1.Solution Ideas

Although the above problems may seem complicated, Let us see through the appearance to perceive the essence,then we will find that the ultimate source of these problems lies in two points:

A.The opacity of the centralized organization in the industry.Under the centralized organization structure,the transaction of the merchant lacks external supervision,and the consumers lack the right to know,it will inevitably lead to high prices and shoddy phenomena.

B.The lack of mutual trust mechanism between different trading entities in different links.There is a lack of trust among trading entities, which leads to increased transaction costs and decreased transaction efficiency.In order to offset this negative impact, the trading entities will improve their own incomes and reduce their own risks through various methods,then there will be various problems.More importantly, the increase of links will further amplify the impact of this lack of mutual trust.

There are two issues that must be resolved to solve: (1) decentralization or weak centralization.Let the main body of the transaction directly connect to improve efficiency.(2)Solve the problem of mutual trust between trading entities, so that the two parties' transactions will not fall into the suspicion chain.However, since the birth of human, the issue of mutual trust has been accompanied by the development of society and has always existed,it is difficult to solve this problem fundamentally by the transformation of traditional technology or model. This requires the introduction of new technical concepts.

2.Solutions

A.The concept of blockchain

The blockchain is an important concept of Bitcoin.It is a decentralized database essentially.In a narrow sense, the blockchain is a chained data structure in which data blocks are sequentially connected in a time-ordered manner,it is an irreproducible and

unforgeable distributed ledger that is cryptographically guaranteed. Broadly speaking, the blockchain technology uses blockchain data structures to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptography to ensure data transmission and access security, and the blockchain technology is a brand new distributed infrastructure and computing paradigm that uses the smart contracts made up of automated scripting code to program and manipulate data.

Popular speaking, blockchain technology is a way for all citizens to participate in accounting. The system which we are using all has a database, if the database as a large book, then it's important for anyone who writes this book. Under the existing technical pattern, you are responsible for accounting for your system. For example, Tencent is responsible for the book of Wechat, Alibaba is responsible for the book of Taobao. In the blockchain system, everyone in the system has the opportunity to participate in billing. If there is any data change within a certain period of time, everyone in the system can make an accounting. The system will judge the fastest and best person of accounting during this period, write the contents of his records to the account, and the contents of the book will be sent to all other people in the system for backup during the period. Everyone in this system has a complete book. In this way, we call it blockchain technology.

B. Technical Features And Advantages

The advantages of the blockchain technology model for people bookkeeping are obvious, includes:

- a. Security: Although the expense of efficiency, great security can be achieved. The entire system does not have a central large books (decentralization), so it cannot be destroyed. Each node is only part of the system, each node has the same rights and has exactly the same books. Destroying some nodes has no effect on the system at all.
- b. Trustworthiness: Once the information is verified and added to the blockchain, it will be stored permanently. Unless someone can control more than 51% of the nodes in the entire system at the same time, the modification of the database on a single node is invalid. So even if a hacker controls a small number of computers to change

information, the system will still refer to most people's opinions to determine what is the true result. The hackers will find it completely meaningless to modify their own books (Because others do not recognize it).

c. High efficiency: Because there are no centralized intermediary agencies, everything is automatically run by the pre-defined process. It not only can greatly reduce costs, but also improve efficiency. And because everyone has the same books, it ensures that the bookkeeping process is open and transparent.

d. Smart contract: The smart contracts is a contract that use computer languages instead of legal languages to record terms. The smart contracts can be executed automatically by a computing system. From the user point of view, the smart contracts are usually considered to be an automatic guarantee account. For example, when certain conditions are met, the program will release and transfer funds. From the technical point of view, smart contracts are considered network servers. However, these servers are not set up on the Internet using IP addresses, but set up on the blockchain, then specific contract procedures can be run on it. The potential benefits of smart contracts include lowering the costs of signing contract, executing contract and monitoring contract. Therefore, this is a significant reduction in labor costs for many low-value transaction-related contracts.

C. The significance of blockchain technology for solving problems

Objectively, the characteristics of blockchain technology have a decisive role in resolving issues of mutual trust in transactions, and it can fundamentally solve various problems existing in the current digital payment market, the specific performance is as follows:

a. Point-to-point transactions: Blockchain technology is based on decentralized features, it makes retail chain point to point transaction can be achieved. From the terminal store to the upstream factory, every transaction entity, is a node in the blockchain, they can trade directly, avoid excessive links, and greatly reduce the cost of circulation.

b. Information transparency: The features of blockchain data information is transparent and unchangeable. Each consumer can see the traceability of the purchased product, which can be traced back to the source of the product. The businesses will no longer sell fake and shoddy products, the quality of products can be guaranteed and the experience of consumers can be greatly improved.

c. Security: In the traditional model, once the central node has problems (such as information leakage), it will bring great threat to the whole system. The security of decentralized blockchain technology is a solution to this problem inherently. The communication is single point of communication between nodes, even if one of node crashes, will not affect the security of the entire system, so the information of user can also be kept confidential (The leaked person is easily found.)

d. Smart contract:

Under the rules of the blockchain definition, each trading entity in the entire industry chain can implement smart contracts automatically by blockchain technology without the need for human intervention. The relationship between the consumer and the retailer can be established, and new retail models (such as unmanned supermarket) will be easier to implement. And under the technical characteristics of information transparency, the phenomenon of price discrimination (Deceive an acquaintance) will disappear completely.

From the above content, we can know that there are some characteristics of decentralization, security, information transparency, and smart contracts. It solve the problem of mutual trust between different parties involved in the transaction fundamentally. This solution is accomplished from the underlying technology, it has a decisive significance for problem-solving and new digital pay retail market.

Chapter 3 Business Model

1. Basic Mode

For problems in the industry, Chengdu Wumeng E-Commerce Co., Ltd. established the HCM project based on blockchain technology. Our goal is to build a platform of decentralization to provide a multi-domain ecosystem to enterprises and individuals in the new retail sector. Under blockchain technology, forming an open, fair and transparent retail consumption chain gradually (P 3-1). In the follow-up, we will also build a public chain to allow more trading entities to build sub-chains on the public chain, and form a decentralized international trade system under blockchain technology gradually.

On HCM, each entity can conduct information transfer, asset transactions, transfers, digital asset allocation equally and etc. These activities are protected and encouraged based on blockchain technology. The HCM can encourage the development of global trade and consumption.



P 3-1 : HCM Model

High efficiency is the most important feature of HCM. The HCM system can handle the payment and redemption of digital currencies efficiently. It enables the user to no longer reduce the experientiality due to payment restrictions in terms of consumer payment and other aspects.

Safety is the gene of the HCM system. The requirements for security run through all aspects of system design, construction, and implementation. Preventing malicious attacks is just a basic configuration. We are not only protect the security of users' funds, but also provide comprehensive protection for users' information.

The effective combination of speed and security, it allows users to securely purchase products and services anytime and anywhere. The HCM system adheres to the concept of openness, cooperation, and win-win cooperation, this will continue to increase cooperation with relevant member agencies and expand cooperation areas. It will continue to deepen cooperation content in the areas of brand marketing, marketing, and new product development, jointly promote business upgrading and promote the compliance and healthy development of the digital payment industry.

2. User Value

This is a very significant value when customers use the HCM, specifically in:

A. Low risk: The HCM covers the range of retail products that consumers use in their daily life, and it can guarantee the user's low risk by cryptocurrency. So there is no risk.

B. High efficiency: In the traditional payment systems and in most cases, there will be delay in payment approval due to high likelihood of fraud, and request to submit numerous documents. But the HCM can immediately approve payments and let experience of both parties (seller and buyer) smooth and easy, don't need to come into even bother.

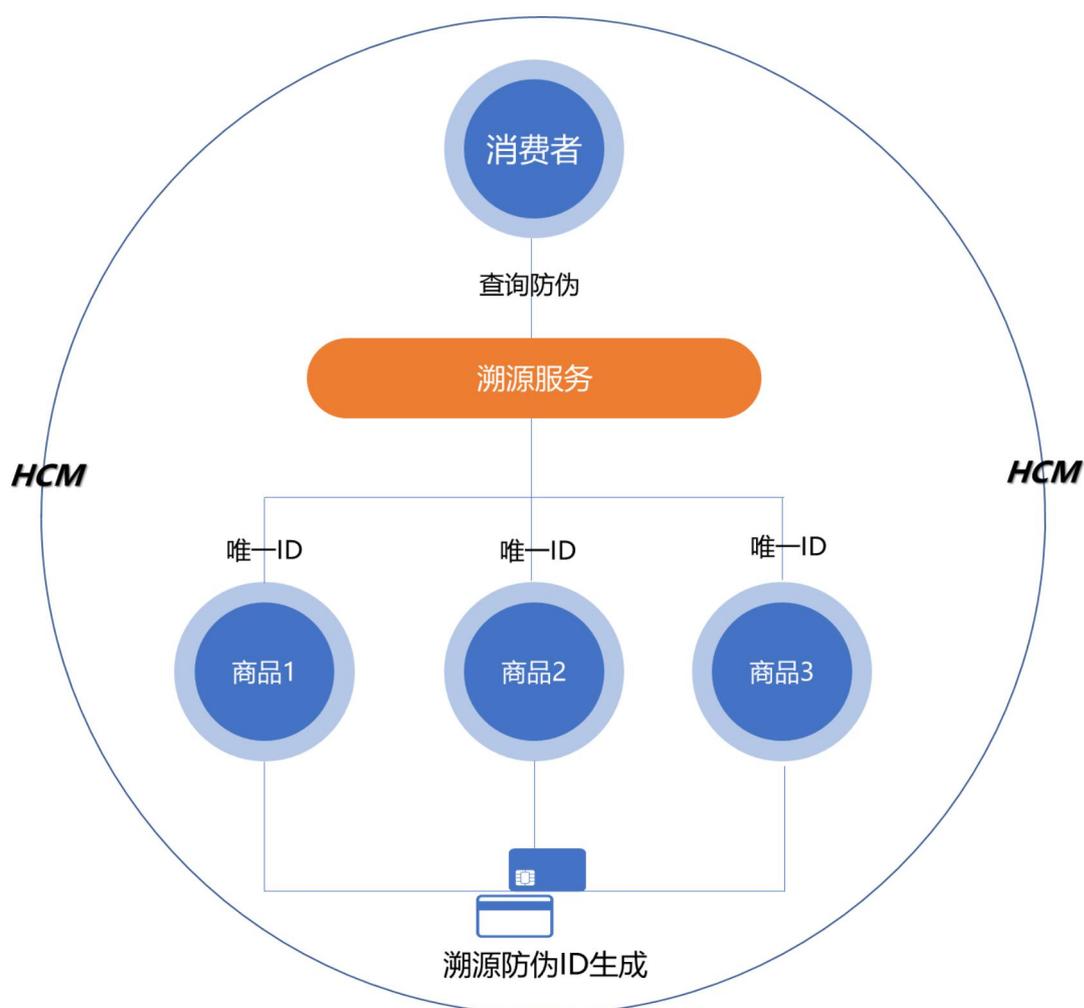
C. Financial security: The HCM use the power of blockchain to let users bid farewell to credit card fraud. The users have absolute control over their private keys and funds, and even we don't have access to the user's wallet. However, the traditional centralized payment plan has a bad record in ensuring the safety of funds.

3. Application Scenario

As a new retail platform supported by blockchain technology, HCM has many application scenarios, as follows:

【Consume payment】 : The ordinary consumers can use HCM to buy goods when they participate in online shopping and offline shopping(such as travel, hotel accommodation, travel and etc.).Because the HCM can help consumers reduce shopping costs and doesn't need to be transferred through intermediate agencies (especially the exchange rate at the time of transnational consumption). In addition, the seller can also save some marketing expenses and use this money to provide personalized, customized promotions and products to end consumers. At the same time, it can also provide consumers with a safe shopping environment by combine blockchain anti-counterfeiting and entity verification

【Traceability service】 : Traceability is the most effective anti-counterfeiting method in the field of commodity sales. There are many loopholes in the traditional traceability technology, such as the opaqueness of the centralized organization, low traceability and etc.. But if use the HCM, it can make the products to achieve informatization, standardization and transparency in the circulation of agricultural products and it also can effectively solve the problems of counterfeiting, label forgery, and public identification difficulties in circulation of agricultural products. The HCM provides consumers with a complete product quality traceability service and to provide the government with full-scale quality supervision data, it creat a new intelligent closed-loop management model for the circulation of agricultural products, from traceability, anti-counterfeit, supervision to counterfeiting. For example, an agricultural product manufacturer is registered and certified at HCM, it will be record the whole process data from raw materials, processing, and logistics circulation information, so that all information of each product is clear. The manufacturers have all date of product information and anti-counterfeit data, so the counterfeit manufacturers have no way to copy, the consumers can rest assured to buy the goods.



P 3-2 : Traceability service

【Financial Service】 : At HCM, the financial institutions can develop applications and provide financial services to businesses and individuals. Through the blockchain, the trading process of all parties can be made more transparent, and it can be more convenient to supervise in the transaction, it can avoid the false trading. In this way, the credit and risk control costs can be reduced. The financial institutions can quickly provide financial services to the needs of businesses and individuals, such as loans, financial leasing, installments and etc., it can meet the financial needs of individuals and small and medium enterprises. At the same time, the HCM officials will also launch financial management services to meet consumer demand for asset appreciation.

【Enterprise Alliance】 : At HCM, the cost of communication between enterprises

is also reduced, because the data can't be tampered and the asymmetry of information is greatly reduced. It solves the problem of distorted information distortion and greatly increases the operational efficiency of the industry chain. The data can flow without loss between the upstream and downstream of the industrial chain. The enterprises can build alliances at low cost, and don't need to waste time playing games, but spend more energy on establishing industry standards, to lay the foundation for expanding the scale and competitiveness of the entire industry.

【Contract transaction】: The HCM provides contractual trading services for both supply and demand by smart contracts, it includes both terminal channels and consumers as well as the supply and demand sides of the upstream of the industrial chain. The supply and demand sides can carry out futures delivery and no-person retailing under the agreed contractual conditions, and they can do it without worry. The HCM can greatly increase transaction efficiency and reduce financial pressure.

【Community service】 : The HCM will build community for the consumers, it can allow consumers to discuss various issues that arise during the purchase and use, sharing the purchase experience. It also can allow consumers to discuss consumer products, stars, price discount and other information in the community, so that let more people participate in the entire platform, forming a good atmosphere.

From the above information, we can know that the HCM plays a huge role in many aspects of the new retail sector. Many problems can be solved by decentralization and transparency mechanisms of the blockchain.

4. Future Development

The development of HCM is defined as the public chain, and the interface will be open later. The trade companies, investment institutions, retail businesses and e-commerce companies can all develop sub-chains on HCM. At that time, the HCM will become a common platform for trade, investment, and consumption of companies and individuals around the world.

As long as there is consumption and trade, there is the value and significance of HCM. In the global trade, investment and consumption, we can imagine the many scene to use digital currency, this will provide sufficient value support for the implement and application of HCM.

Chapter 4 Technical Realization

1. Technology Architecture

A. HCM public chain

The HCM Public Chain is committed to developing new ecosystems other than Bitcoin and Ethereum. Through the perfect design to achieve compatibility with Bitcoin's long-term technology evolution and Ethereum virtual machines, and industry-oriented. Through the development strategy of APP, bring the technological advantages of blockchain to users of different industries and ordinary Internet. In addition, the HCM public-chain system focuses on the practical application of smart contracts, it will be designed through the perfect Oracle and Identity sections to give a compliant and open blockchain technology pilot site for the traditional Internet companies (Such as finance, Internet and etc.). In addition, the HCM system focuses on the development of decentralized applications. By attracting third-party developers to join together to provide decentralized applications for mobile users, for all third-party applications developed based on the HCM system, the HCM will reward developers with a comprehensive evaluation system.

The initial design goal of the HCM system are: The first POS smart contract platform compatible with BIP protocol, and through the introduction of Identity and Oracle and Data feeds, in compliance meeting the regulatory needs of different industries. On the HCM platform, we will develop and innovate through continuous blockchain technology and attract third-party developers, industry users, and general users to build HCM platforms and ecosystems together.

B. Model comparison

a. UTXO model analysis

In Bitcoin's network, the UTXO (Unspent Transaction Output) is the basic unit of Bitcoin transactions. Through the input and output of transactions, the Bitcoin network changes money into a data structure. Different from credit card payment, credit card payment must be transmitted in the encrypted secure network, but Bitcoin data can be transmitted in any network (such as WIFI, bluetooth, NFC, table and etc.) that maybe is

not necessarily secure. The UTXO can be any integer multiple of (1×10^{-9} BTC).

The UTXO can be any number less than 21 million, but once the UTXO is created, it can only be spent as a whole. If the BTC required for a transaction is less than the value of a UTXO, then the UTXO will still be spent as a whole, and a UTXO of change will be formed.

The UTXO can be seen as the Bitcoin currency unit that is locked by the owner of the private key and recognized by the entire Bitcoin network.

In the UTXO model, UTXO consumed by a transaction is called transaction input, and UTXO created by the transaction is called transaction output. In this way, it will consume and create new UTXO in the transaction chain by a certain amount of bitcoin transfers between different private key owners. A Bitcoin transaction will be unlocked UTXO by the owner's private key, and unlocks and create UTXO by use the Bitcoin address of the new owner. At the beginning of the Bitcoin network, the miners will get Bitcoin by a special transaction type-Output of transactions created by Coinbase transactions (the transaction was not entered), the miners can use this Bitcoin to create other UTXO.

UTXO is tracked by a full-node Bitcoin client in a database stored in memory, database is also known as "UTXO Set" or "UTXO Pool". One or more outputs are consumed from the UTXO pool when the new transaction is built, while the Bitcoin network monitors all available UTXOs in millions. There is no concept of "bitcoin balance" in the bitcoin network in the world. Because only all unexpended UTXOs are logged on the Bitcoin network. The concept of Bitcoin's balance is more derived from the Bitcoin wallet client, the Bitcoin wallet calculates the user's balance by sweeping the blockchain and aggregating all UTXOs belonging to the user.

In addition, about the issue of transaction costs, we can calculate the transaction cost of a transaction by calculating the difference between the input and output.

$$\text{Bitcoin network transaction fees} = \text{Transaction input sum} - \text{transaction output sum}$$

Transaction input and output data structures in the Bitcoin network:
 Bitcoin transaction input data structure

Bitcoin transaction input data structure		
Bytes	Field meaning	Remark
32 bytes	Transaction	Pointer to UTXO
4 bytes	Output index	UTXO index to be expended
1-9 bytes	Unlock script size	Unlock script bytes
Lengthen bytes	Unlock script	Unlock script
4 bytes	Serial number	Unused transaction replacement function

Bitcoin transaction output data structure		
Bytes	Field meaning	Remark
8 bytes	Bitcoin quantity	Unit is BTC
1-9 bytes	Lock script size	Lock script bytes
Lengthen bytes	Lock script	Expense output needs to meet the conditions of the script

In the UTXO model, we can clearly trace the history of each transaction through an open book and can be completely transparent and. In addition, the UTXO model also brings certain parallel processing capabilities, it can initiate multi-address to multi-address transactions, it brings some reference for scalability. In addition, the UTXO model also brings a certain degree of privacy. The user can use Change address as the output address of UTXO. But UTXO is stateless, we will implement smart contracts based on the UTXO type through a series of innovative designs.

b. Account model analysis

Unlike the UTXO model, the Ethereum has an account system. In the white paper of Ethereum, we can know the account system of Ethereum:

In the Ethereum system,

The state is composed of objects called "accounts" (Each account consists of a 20-byte address) and state transitions that transfer value and information between two accounts. The Ethereum's account contains four parts:

Random number: it is used to determine the counter that can only be processed once per transaction

The current Ether balance in the account

The account code of the account, if any

The account storage (Default is empty)

The Ether is the main encrypted fuel inside Ethereum, it is used to pay transaction fees. In general, the Ethereum has two types of accounts: all external accounts (private key controlled) and contract accounts (contract codes controlled). All external accounts have no code, and people can send messages from an external account by creating and signing a transaction. When the contract account receives a message, the code inside the contract is activated, allowing it to read and write internal stores, and send other messages or create contracts.

In the Ethereum system, the account balance is recorded through a stateful account system. The increase/decrease in the balance of each account is more like the bank accounting in the real world. Each time a new block is created, it can affect the global state. Each account has its own balance, storage, and code area. In this way, the contract can call the account or address, and store the corresponding execution result in the storage area.

In the current Ethereum account system, with client/HCM, only one-to-one transfers are possible, which means that you can only transfer from one account to another at a time. Although smart contracts can be sent to more accounts, these internal transactions can only be displayed on the user's account balance, but it is difficult to track Ethereum's public books.

The UTXO model of the Bitcoin network ensures the continuity and traceability of Bitcoin transactions, it is also the core design of the Bitcoin architecture. Considering the network effects of Bitcoin and the advantages of the UTXO model, in the HCM public chain system, our first step was decided to take a UTXO-based model.

c. Consensus mechanism

The consensus mechanism in HCM is designed to be modular and can be plugged and unplugged like a plug-in. It can apply different application scenarios of public and private chains.

In the selection of HCM consensus mechanism, according to the principle of technical reliability and the principle of decentralization, We finally selected the Proof of Stake-based consensus mechanism as the basic consensus mechanism of the public chain. In the HCM-based alliance chain, we use the consensus mechanism that combines the Proof of Time and Raft protocols, it can provide services for industry customers.

Before in the community there are many discussions about the consensus mechanism, from POW to POS to DPOS, to the BFT consensus mechanism of HyperLedger. The essence of the consensus mechanism is how to pass some algorithms in a distributed system and finally obtain the consistency of the data. Discussions on consensus mechanisms will eventually return to the consistency of distributed systems in the computer field. There are a lot of research and achievements in this area before, for example, the FLP theorem and the CAP theorem in distributed systems guide how people design consensus mechanisms based on specific needs.

In Bitcoin's network, the miners participate in the verification process of the Bitcoin network through Bitcoin's full client, and the miners get the Hash value randomly by way of proof workload. When the miner calculates the Hash value and satisfies certain conditions, we say that the miner dug a block. It mean:

$$\text{Hash}(B_Header) \leq MD$$

The Hash function represents 2 SHA256 calculations. The range of values is $[0, M]$, D is an integer of $[1, M]$. The Bitcoin network's SHA256 mining algorithm allows each node to quickly verify the validity of the block, and each block of BlockHeader changes with Nonce and extra Nonce. The difficulty of the overall mining will be dynamically adjusted according to the total power of the network. According to the consensus agreement, when the network is forked, we will select blocks that contain more work as valid blocks.

After that according to the different of mining algorithm, There are also other Proof of Work algorithms, for example, the Script algorithm of Litecoin and the X11 algorithm of Darkcoin. The original intention of the design is to resist the

centralization of computing power to ensure the decentralization of the network.

The codes of Proof of Stake used in the community are mostly forked in PeerCoin, and PeerCoin is modified based on the very old version of Bitcoin code and cannot reflect the features of the BIP protocol and the integrity of the code in recent years.

In the HCM's public chain system, the basis of our consensus agreement is Proof of Stake. And we will develop and deploy the Proof of Stake consensus protocol based on the latest Bitcoin code.

In the HCM's public chain system, will choose some tradeoffs of Proof of Stake: the degree of decentralization, the difficulty of nodes participating in billing and network maintenance costs. In the Huabo Union Chain System, involving identification and trusted networks, more often in a restricted group, the periodic random selection of billing nodes. We will combine the Proof of Time and Raft protocols given by HCM for the federated chain system to design corresponding consensus protocols. The specific design ideas see HCM Yellow Paper. The design goal is Block time: 250 milliseconds Verification time 750 milliseconds - 3 seconds, it can meet the characteristics of scalability and low latency.

d. Contracts and virtual machines

In this section, we mainly discuss the contract, the execution environment of the contract virtual machine and the concept of simple contract given by the HCM system.

In this section, the Contract here we refer to Blockchain Related Contract, and divided the blockchain contract into Smart Contract and Simple Contract.

Smart Contract: The blockchain contract code is executed by the virtual machine and does not focus on the input of data under the chain. The blockchain network itself provides contract trigger conditions to complete the execution of the contract. Simple Contract: The block contract code is executed by the virtual machine, focusing on the input of the data under the chain (Oracle and DataFeeds), and the execution of the contract is completed through the common input of the chain data and the block chain network as a trigger condition. In the HCM system, considering the actual use of the

contract, we will design a complete service of Oracle and DataFeed to push the blockchain contract to the actual business application scenario.

Let's look at the simplest contract types in the bitcoin network: Multi-signature.

In Bitcoin's 2 of 3 multi-signature contracts, the participants agreed to put Bitcoin's funds into the input of a transaction. Through a multi-signature transaction, the cost of this currency fund usually requires the consent of at least 2 parties to spend this funds. This type of contract requires an arbiter to participate as a third party because of the two outcomes of a multi-signature contract. The first result, and all issued their own signatures. The second result is that one of the parties does not agree to issue a signature, resulting in the inability to use the funds. At this time, the arbitrator must be involved and the funds should be released to the party he thinks is correct. In this contract process, we can design Mediator to automatically provide Oracle with a trusted source of data, and actually obtain the corresponding data from the outside, instead of fetching the input data for contract execution from the blockchain network itself.

Profit from Ethereum contract execution environment EVM, the creation and execution of contracts in Ethereum is very simple. However, the implementation of the above contract at Ethereum at this stage did not involve too much intervention in external data, which also caused limitations in the display of business scenarios. On the HCM contract platform, we will abstract external data and interventions into Oracle and DataFeed, and we expect to bring blockchain contracts to specific business scenarios through simple contract forms.

The DAO events in Ethereum expose potential security factors that may exist in the design of smart contracts. Because the smart contract on Ethereum is deployed once, the EVM will execute the contract code step by step through the predefined addressing pointer and OP_CODES, and the global state will be converted according to the execution result of the contract. Software development in the real world is usually accomplished through multiple iterations. However, once the smart contract cannot be implemented through iterative improvement, this feature is in line with the blockchain criteria, but it is very different from the social norms and business rules in

the real world. So in the HCM system, in addition to supporting Ethereum smart contracts, we will establish a bridge between the real world and the blockchain. By introducing the rules under the chain, we will write the simplest and smallest set of contract requirements on the blockchain, for example, parties to the contract and authorized parties, and through the input of the chain data to trigger the execution result of the contract, and to upgrade the contract code through the arbitration under the chain. The original intention of the simple contract is to introduce social rules and business rules to the blockchain, making it easier for the blockchain technology to meet the needs of the real world.

e. Identification and privacy

The HCM system will manage users on the HCM platform through smart contracts. The HCM system will provide an optional identity module, and identity is a prerequisite for the blockchain system to be able to dock to the financial system.

In the HCM system, we will distinguish between identity and non-identity customers.

The HCM system developers will develop code based on the corresponding identification smart contract and open source code to third parties. Through the introduction of third-party credit bureaus, customers authenticated by the smart contract will have more priorities in the HCM system.

For example, in the DAPP for financial services in the HCM system, the identity verification customers will get more privileges.

About privacy, because the HCM system is compatible with the UTXO model, ZeroCoin is an encrypted transport protocol based on the UTXO model.

Currently Zcash is in a public beta. We will provide more privacy protection for smart contracts and transactions in the HCM system through integration with the Zcash protocol.

2. Technical Features And Advantages

Through a large number of data test analysis, HCM can be achieved in terms of performance: second-level transaction verification, mass data storage, high throughput

and node data is quickly synchronized. Achievable in terms of scalability: Cross-link transmission and Rights control strategy. At the same time, it provides secure private key access services and privacy protection solutions.

A. Performance

a. Fast transaction verification

Through the optimization of key links such as signature algorithm, account structure, data manipulation, serialization, consensus mechanism, and message diffusion, the HCM blockchain can be easily verified in seconds. Meet the user experience of most blockchain application scenarios.

b. Mass data storage

The double block bookkeeping mode of the blockchain allows continuous accumulation of historical data during long-term operation of the system. The HCM blockchain uses the mechanism of separate storage and storage of hot and cold data in traditional financial systems to achieve effective storage of massive data. Old transaction data, inactive asset data and other information can be stored using big data storage platform (such as Hadoop, meet the PB level of data storage).

c. High throughput

The essence of blockchain is a distributed shared billing technology. Its distributed features are mainly distributed consistency rather than distributed concurrency processing. In order to ensure the consistency of data and prevent the Byzantine issue, certain specific links can only be implemented serially and not in parallel. Through long-term testing and optimization practices, the processing performance of the HCM blockchain has been able to meet the needs of 10,000 TPS. If the re-introduction of Off-Chain and other mechanisms, can further significantly increase transaction throughput.

d. Node data is quickly synchronized

The HCM supports mirroring mechanism, it can regularly mirror the local ledger, and implement a convenient rollback mechanism. Under a unified consensus, it can specify image tags to roll back. At the same time, by shortening the cycle of adding new nodes into operation, it is only necessary to synchronize the latest image

with a small number of recent transaction sets to integrate into the network and participate in consensus verification.

B.Extensibility

a.Cross-chain technology:Cross-chain technology is the key to the realization of value networks. It is a bridge for the expansion and connection of blockchains.As the HCM with a global payment network as its core, it is very important to connect with other blockchain projects.HCM developed its own cross-chain technology with the following technical highlights:

1.Bidirectionally anchored side chains:Sidechains are a convergent way of achieving the goal of cryptocurrency financial ecology, rather than excluding existing systems like other cryptocurrencies.The HCM uses two-way hooking technology,the purpose of the side-chain protocol is to achieve bi-directional anchoring so that the digital currency of the HCM can use the side-chains in the main chain and the side chain.We can easily establish a variety of intelligent financial contracts, stocks, futures, derivatives and so on.

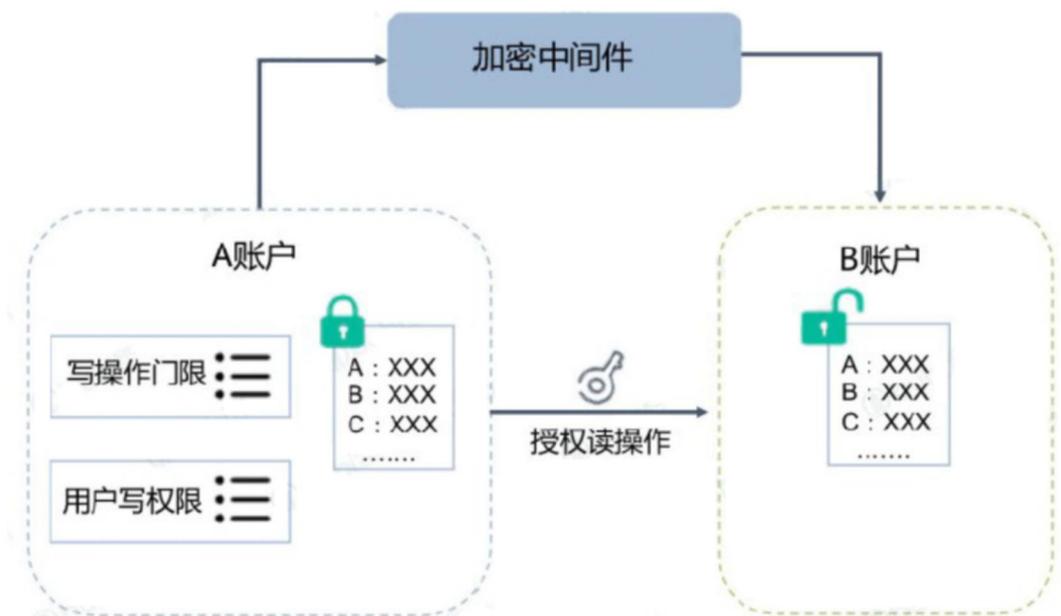
2.Relay technology:This is a way of distinguishing between the way a party initiates and executes a transaction and the way in which the transaction party records it.Many verifiable, globally-synchronous data architectures are built on this foundation.These data structures are parallel chains or side chains, which are adjusted according to individual requirements, or different functions are set for different chains to achieve better scalability and efficiency.Finally let HCM communicate directly with any chain.

3.Fair technology:The HCM integrates all data in the network into items or chains.User data is stored in the entries, and the chain and the entries form an interactive collaboration, so that their data storage does not rely solely on a single blockchain of bitcoin books, but as an effective way to link multiple chains.

b.Rights control strategy

Provides two types of permission control policies for writing and reading data information.Write permission for data information, set multiple users under the same account, and set corresponding rights for different operations to meet the use

scenarios of multi-signature control. Read permission for data information, the user can grant and withdraw the operation authority for data of a single user or user group, and the user group can be flexibly configured by the user. The data includes user account information, transaction information, etc. The granularity can be detailed to each attribute field of the transaction or account.

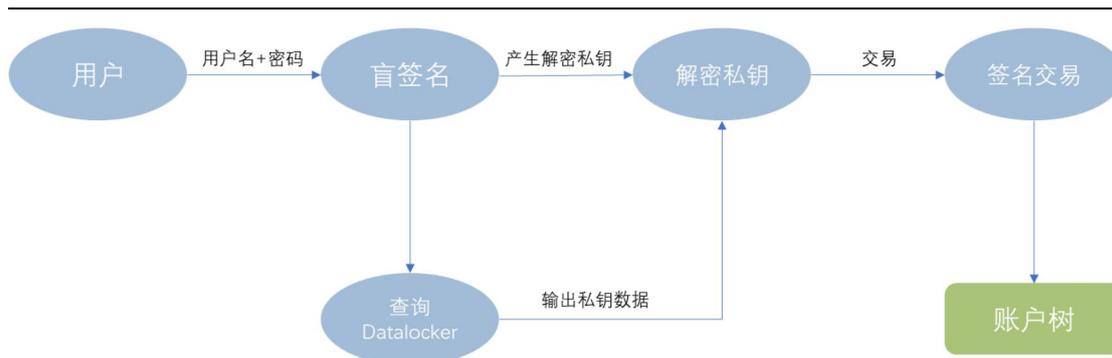


P4-1 : Rights control strategy

C. Safety aspects

a. Secure private key access

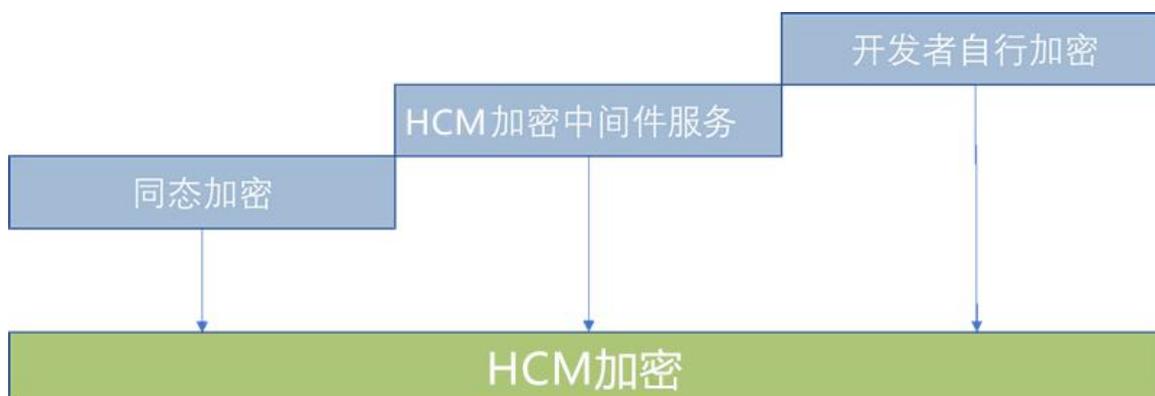
In order to facilitate users to use blockchain product services, in addition to the traditional mechanisms for client generation and saving, HCM also provides two solutions: web hosting access and private key hardware access (U-key). Web hosting access, that is, the user name and password are mapped to private keys by specific algorithms and stored on the server. The private key stored on the server is encrypted, and the private key can only be decrypted on the client. The hardware private key is to meet the needs of the industry. This set of algorithms surpasses the current new private key control authentication algorithm for all main chains.



P4-2 : Secure private key access

b. Multiple privacy protection

The HCM can provides multiple privacy protection features. First of all, the underlying blockchain provides homomorphic encryption. All user data is encrypted and stored, only visible to the user. Second, HCM provides encrypted middleware services that users can choose based on business needs. Finally, the upper application can encrypt the data when it is entered, and the HCM platform is responsible for writing and reading user-generated encrypted data.



P4-3 : Multiple privacy protection

Chapter 5 Core Values And Differentiation Presentation

HCM is currently one of the few projects that combines the physical content with the blockchain. The following is core values and differentiated advantages of our project:

1. Physical Asset Endorsement

There are some difference between our blockchain project and the vast majority of technology-driven blockchain projects. The HCM relies on entity companies as endorsement and creation. The HCM initiated by entity company which named Chengdu Wumeng E-commerce Co., Ltd, they have hundreds of chain stores in the Operations Center of Sichuan, and continue to expand. The users download a digital wallet, and apply for a new wallet address in the HCM official accounts or leave a message in the applet, then the operator will automatically send the digital currency to the user's wallet, the users can shop by use these digital currencies in physical stores under the HCM line. The HCM full use of the technical characteristics of the blockchain, in the characteristics of traceability and peer-to-peer trading, there is no fake on HCM, and the price of goods on HCM is more than 50% cheaper than in the market. Therefore, compared with other blockchain projects, the digital currency issued by HCM have the space to preserve the value of physical assets.

2. Financial Services

The function of HCM is not only solve the problem which the concerns of consumers in the new retail, and saves money for consumers, but also allow consumers to make money. The HCM team will soon launch a wealth management service. The users can enjoy secure financial services after purchasing digital currency. The HCM team will cooperate with large funds to obtain stable revenue returns to users by decentralized investment strategies.

Chapter 6 Release notes

1.HCM Digital Currency Introduction

The HCM digital currency is the blood that drives the decentralized HCM ecosystem. In the main chain of HCM , we will encourage companies to develop sub-chains. At that time, between sub-chains the data exchange, implementation of smart contracts and all aspects of asset and information data exchange will consume HCM digital currency.The HCM digital currency will become a common currency on the ecosystem of the entire chain.

2.Issuance Plan

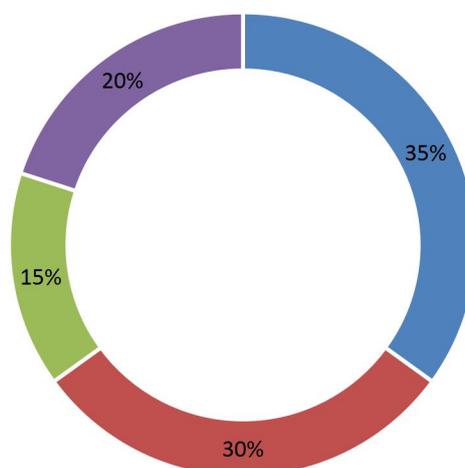
The total circulation of HCM are 1 billion piece, The distribution is as follows:

Table 1 : HCM Digital Currency Issuance Program

Proportion	Quantity	Distribution plan	Remark
14%	140 million	Presale	Pre-sale to relevant private placement agency, fundraising is used for HCM Operation, including development, marketing, operations, reserve funds and etc.
10%	100 million	Team retention	The founding team holds the currency,the lockup period for 4 years,and unlock 25% per year.
10%	100 million	Strategic cooperation	Business cooperation and marketing for HCM project partners.
6%	60 million	Community operation and maintenance	Building an open source community for community operation and maintenance, user rewards, and support for third-party developers,and organize various events to establish HCM Ecology
20%	200 million	Industrial chain exchange circulation	For the circulation and exchange of digital currency in the industrial chain.
40%	400 million	Mining reward	Calculate mining manpowere ,rward to the miners

3.Fundraising Use

The use of HCM private funds includes technology research and development, market development, daily operations, project reserves and etc.The specific proportions are as follows:



- 技术研发 (项目持续健康运作和后续技术开发运用)
- 市场开拓 (市场前期运营和公关团队宣传)
- 日常运营 (平台日常维护, 团队运营, 财务审计等)
- 项目储备金 (项目运营特殊事务以及各方面应急支出)

- Technology R & D(Sustained and healthy operation of the project and the Follow-up technical development and application)
- Market Development (Market pre-operation and PR team promotion)
- Daily Promotion (Daily maintenance of the platform,team operation,financial audit and etc.)
- Project Reserve(Project operation special affairs and contingency expenses in all aspects)

P 6-1 : Private equity use

Chapter 7 Governance structure

The HCM project uses the form of foundation to govern.

The Foundation is dedicated to the construction and governance of HCM. The main target of foundation is to ensure the sustainable development of the HCM project, and ensure the fundraising security and management effectiveness. The organizational structure of the HCM foundation is composed of Decision committee, foundation Self-Governing Committee and executive committee. The governance structure includes the operational procedures and rules of daily work and special situations.

In order to avoid inconsistencies in the directions and decisions of community members even make the community to be split. The Foundation explains the general and privileged matters of manage the community by make a good governance structure. The design goal of the foundation governance structure is to keep the sustainable development, decision efficiency and money management compliance of the platform. In the foundation, the decision-making committee exercises daily powers.

After the expiration of the term decision-making committee, five core members of the decision-making committee will be selected by the community vote. The selected core personnel will make important and urgent decisions on behalf of the foundation, and he will need to accept credit investigation during his tenure. At the beginning of the foundation, in order to facilitate the rapid progress of the project, the first decision-making committee members will be composed of team members and early investor representatives for a term of two years. When the end of the term of the members of the decision-making committee, the community will vote to re-elect. The decision-making committee consists of 5 members, of which the team represents 3 people and the early investor represents 2 people. All decisions were made using the 3/5 multi-signature system.

Chapter 8 Team Introduction

All our team members are senior experts in the relevant fields of the industry, and they have a wealth of resources and experience. In addition, a lot of work has been carried out in the early stage of the project and the results have been outstanding. Details are as follows:

Alexander Zhou (Chief architect)

Alexander is a core researcher of blockchains and digital currencies and internet finance businesses in international consulting companies. He has deep industry expertise and extensive consulting experience, committed to solving a series of strategic and cognitive issues for the company, and he has served clients, such as Tencent, Alibaba, Anda Insurance, Goldman Sachs, Haitong International, Price Waterhouse Coopers and others. Alexander has been engaged in blockchain research for 3 years and he has a unique understanding and know of blockchain and digital currency. His views are deeply appreciated by senior executives of traditional financial companies and practitioners of the blockchain industry, and he has promoted the Chinese community cognitive changes of block chain technology and digital currency. It is clear that the blockchain and digital currency are cored by Distributed Database, and the consensus of the underlying architecture of P2P Network, Consensus Design and other technologies. Alexander is convinced that ICO is the best way to transform the current financial industry's cumbersome financing methods and processes. With its efficient and low-cost financing functions, ICO will greatly promote the development of human science and technology based on blockchain technology, so as to better benefit the society, and give the investors of digital currency projects a quick, safe and stable return.

Alex Feng (Director of the underlying architecture)

Alex is a senior technical person in the domestic Internet field. He has many years of experience as an architect in Alibaba and Tencent. He is well known for cloud computing, low-level system architecture and operating system development, and he applied for a patent of virtualization and cloud storage. Alex is proficient in a

variety of computer languages,he has deeply customized solutions and developing an implementation plan for Tencent cloud architecture & big data.

David Li (Senior engineer)

David is a Dr. Computer from Princeton University in the United States. He has worked at Microsoft, he has extensive experience in program development and he has involved in various Microsoft operating system upgrade maintenance.David has more than five years of experience in App development.

Pavel Yushchenko (Encryption algorithms and distributed data engineers)

He is a programmer and software architect with more than 15 years of experience.He graduated from Moscow State University with a master's degree in computational science and mathematics. He created network and security-related services,he even created his own programming language and cross-platform compiler for signature-based intrusion detection systems.As an advocate of strong encryption currency,he promotes the practical application of blockchain technology and assimilated big data and artificial intelligence.

Upadhi Kabra (Chief Financial Officer)

Upadhi was an executive director in JP Morgan Chase ,he is an MBA of Wharton. He has many years of practical experience in financial product management, risk control, strategic analysis, project execution, and money management.

Bob Song (Chief Operating Officer)

He served as director of marketing for Silicon Valley startups,and he has a deep understands of the way of hacker growth.He can accurately grasp market trends and positive direction,and he can use a variety of marketing and psychology tools flexibly,such as hunger marketing, viral marketing, hacking growth, and he can control the key time point of event marketing

【Project Consultant】

Luke Taylor

He is Professor of Finance at the Wharton School of the University of

Pennsylvania, Doctor of Finance at the University of Chicago, Senior Financial Expert at McKinsey, and he was an off-site consultant for several CEOs and hedge funds and venture capital funds. Dr. Taylor has unique insights and in-depth research of financial product innovation research, and he has published many academic research papers in the Journal of Finance, Journal of Financial Economics, and Review of Financial Studies, he also wrote articles for Forbes and the Wall Street Journal.

Peter Lee

He graduated from the University of Southern California. He is the major partner of Cofound.it, a well-known blockchain investment company, during his tenure, he provided strategic support to many well-known blockchain companies around the world. Before he joined in Cofound.it, he was engaged in strategic consulting for Apple, Accenture, and AIDS.

Genevieve Leveille

She is technical consultant of Estonia blockchain, and the founder of digital currency influence organization. She graduated from Columbia University in the United States, she has experience working in the information technology and services industry. And she has a strong entrepreneurial spirit, she is good at cash, market risk, circulating fund management, treasury and business transformation.

Andreas Grosjean

He is a member of the board of Ming Le Sports AG, the chairman of the supervision committee of GoldRooster AG and a member of the Munich Stock Exchange. He graduated from Maximilians University in Ludwig, Munich, and he has experience working in the investment bank. He is proficient in computer knowledge, entrepreneurship, venture capital, securities and stocks.

Chapter 9 Risk Warning and Disclaimer

- As a new investment model, digital asset investment has a variety of risks. The potential investors need to assess the investment risk and affordability of themselves carefully.
- The document is used to guide the progress of the HCM project and it is just used to convey the information, it does not constitute the relevant opinions about buying and selling HCM digital currency. The above information and analysis does not constitute investment decision. This document does not constitute any investment advice, investment intentions and abetting investment
- The document does not constitute and understood as provide any buying or selling, any invitation of trading behavior and any form of securities act, it is also not any form of contract or commitment.
- The relevant intention users have a clear understanding of the risks of the HCM project. Once the investor participates in the investment, he understands and accepts the risk of the project, and he is willing to bear all corresponding results or consequences personally.
- Our project team are not responsible for any assets losing of participating in the HCM project.
- Project risk :
 - Policy risk: Blockchain technology is early stage, the national will have some regulatory policy to the blockchain project, it will be ambiguity. The projects may have changes about operational entities and operations management.
 - Fluctuation risk: The HCM digital currency is not an official currency, it is just a digital currency in blockchain project, and the fluctuations of price are huge. It requires the investors to have a certain mental capacity.
 - Technical risk: For the continuous development of the blockchain technology, we can not guarantee the avoidance of technical loopholes and hacking attacks in the project operations.

- Team risk: We can not guarantee that the departure of core personnel due to stress, physical and personal factors during the development of HCM , but we can guarantee that team will make the project more stable develop.