GLOBAL VALUE CHAIN

The Application of the Underlying Public Chain

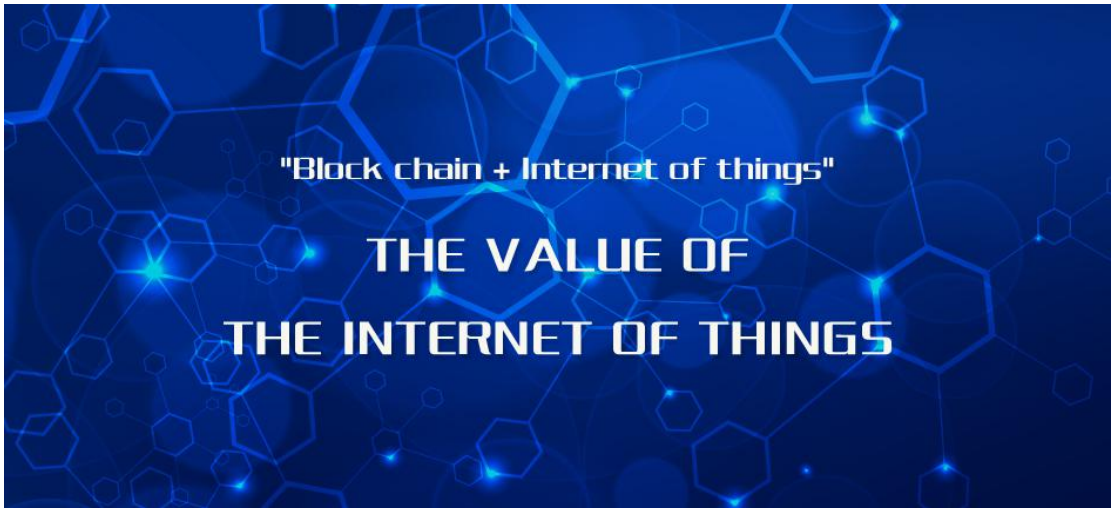
of the Internet of Things

Global Value Chain (GVC) Team

April 2018

Contents

Part Ⅰ creates a new era of value Internet of Things



The 21st century is an era of rapid economic development and an era in which new technologies lead society to change. In the era of rapid development of the Internet, people's collaboration and communication have broken through the limitations of time and space, and the world has become an overall interactive platform.

With the rapid development of society, the Internet industry has also been continuously renovating. In the previous years, the development of the Internet has entered the "Internet+" era of the Internet 2.0 era. This stage is the economy of "Internet + traditional industries" promoted by the innovation of knowledge society 2.0. The new form of social development provides a broad network platform for the reform, innovation, and development of all walks of life.

In the past two years, under the impetus of the "Internet+" development wave, the information age has entered an unprecedentedly important stage of development,

and the Internet can achieve “connected objects”. This stage is known as the development of the world's information industry following the computer and the Internet. The third wave of "Internet of Things", the Internet is striding toward a new era of development.

However, from the Internet to the “Internet+” and then to the Internet of Things, the problems of localization of information dissemination (centralization) have not been solved at all stages. Under the current centralized architecture, the Internet of Things is difficult to accomplish truly autonomous collaboration and effective transactions because the parties involved in this collaboration and transaction often belong to different stakeholders and have complex and difficult-to-determine trust relationships. Therefore, current collaboration and transactions of IoT devices can only be conducted under the same trust domain; that is, devices for collaboration and transaction must be provided or authorized by the same IoT operating service provider, which greatly reduces the application of IoT. commercial value.

In this situation, we propose "value Internet of Things," focusing on the introduction of blockchain technology into the Internet of Things and addressing the centralization issues facing the development of the Internet of Things. Blockchain is a decentralized transaction record storage technology. It is based on cryptographic principles. With a distributed peer-to-peer network, it realizes the permanent storage of ordered transaction records, which cannot be deleted and tampered with, and is open and traceable. Therefore, it is Recognized as the only

choice to meet the above challenges. In the ecology of the blockchain, people can securely conduct transactions without having to establish trust in advance, because each transaction is recorded in the blockchain's "public account book" and is well documented. It can perfectly solve the Internet. The problem of trust and equity in the virtual world.

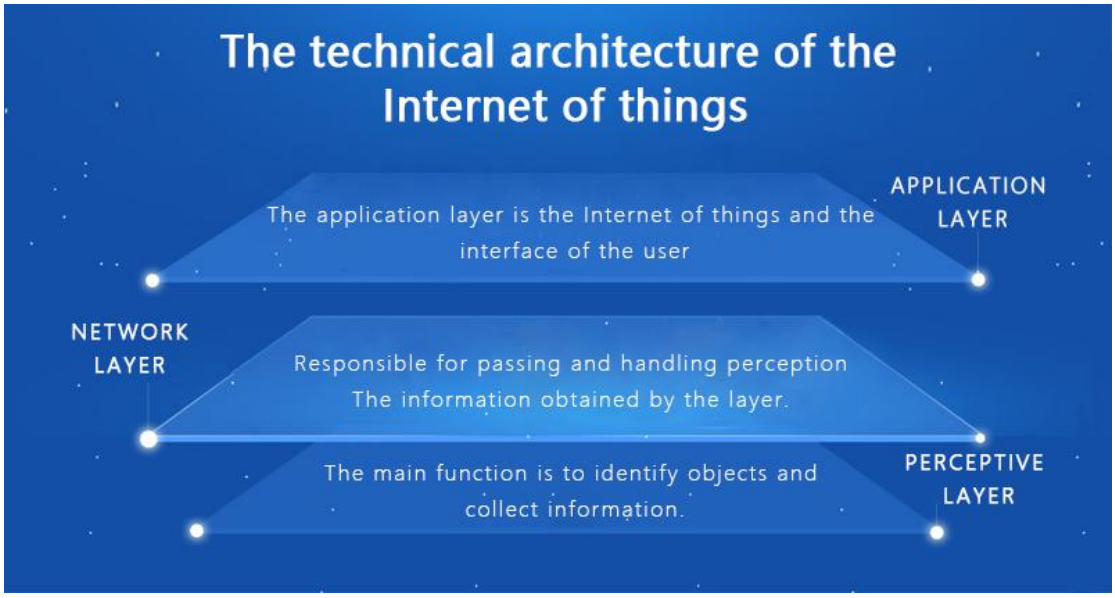
1.1 Internet of Things

1.1.1 Interpretation of the Internet of Things

Internet of things (IoT) is the Internet connected with objects. Its core consists of two layers of meanings. First, the core and foundation of the Internet of Things is still the Internet, which is an extension and expansion network based on the Internet; Second, its user end extends and expands to any item and item for information exchange and communication, that is, the object rests.

1.1.2 Internet of Things Technology Architecture

From a technical architecture perspective, the Internet of Things can be divided into three layers: the perception layer, the network layer, and the application layer.



Sensory layer: It consists of various sensors and sensor gateways, including CO2 concentration sensors, temperature sensors, humidity sensors, two-dimensional code labels, RFID tags and readers, cameras, GPS, and other sensing terminals. The role of the sensory layer is equivalent to the nerve endings of the human eye, nose, nose, throat, and skin. It is the source of information for the Internet of Things to identify objects and collect information. Its main function is to identify objects and collect information.

Network layer: It is composed of various private networks, the Internet, wired and wireless communication networks, network management systems, and cloud computing platforms. It is equivalent to the human nerve center and brain and is responsible for transmitting and processing information acquired by the sensory layer.

Application layer: It is the interface between the Internet of things and users (including people, organizations, and other systems). It is combined with

industry requirements to realize the intelligent application of the Internet of Things.

1.1.3 Development of the Internet of Things

The practice of the Internet of Things can be traced back to 1990 when Xerox's online Coke vending machine, Networked Coke Machine.

In 2003, the United States "Technical Review" proposed that sensor network technology will be the top ten technologies that will change people's lives in the future.

On November 17, 2005, at the World Summit on the Information Society (WSIS) held in Tunisia, the International Telecommunication Union (ITU) released the "ITU Internet Report 2005: The Internet of Things," quoting the concept of the "Internet of Things." The definition and scope of the Internet of Things have changed and the coverage has been greatly expanded. It no longer refers to the Internet of Things based on RFID technology.

After 2008, in order to promote the development of science and technology and seek new growth points for the economy, governments of various countries began to pay attention to the next generation of technology planning and have focused on the Internet of Things. In China, the Second China Mobile Government Affairs Seminar "Knowledge Society and Innovation 2.0" held at Peking University in November of the same year proposed that the development of mobile technology and Internet of Things technology represents the formation of a new generation of

information technology, and has driven the economic and social development. The innovation of the innovation form has promoted the formation of the next generation of innovation (innovation 2.0) with the user experience as the core for the knowledge society.

In China, the Internet of Things has been listed as one of the seven strategic emerging industries by the Twelfth Five-Year Plan, and is the main force that will lead the Chinese economy into a magnificent turn. The industry scale of the Internet of Things will reach 600 billion during the 12th Five-Year Period. The research agency forrester predicts that it will be within 10 years. The Internet of Things will become a trillion-dollar industry that is 30 times larger than the Internet.

The Internet of Things has a wide range of applications, including intelligent transportation, environmental protection, government work, public safety, safe home, smart fire protection, industrial monitoring, environmental monitoring, elderly care, personal health, flower cultivation, water system monitoring, food traceability, enemy investigation and intelligence Collecting and other fields.

Since 2013, the integration of sensor technology, cloud computing, big data, and mobile Internet has developed. The application of the global Internet of Things has entered a substantive stage of advancement. Countries and regions such as Europe, the United States, Japan, and South Korea made important progress in the technology and application of Internet of Things. Informationization, digitization, and intelligence have become the direction and direction of a new round of technological revolution.

1.2 Blockchain

1.2.1 The rise of blockchain

Starting from getting rid of third-party constraints

Earlier, people viewed the blockchain as a ledger on a peer-to-peer network. Since the beginning of each transaction, all transfers and transactions will be recorded on the "block". Blocks and blocks are connected end to end. The chained structure is published to all nodes on the network, and consensus is formed between the nodes. Node members can review related transaction records based on their permissions, but any individual node cannot easily control and change data across the entire network.

This design was derived from the 2008 issue of Bitcoin: A Point-to-Point Electronic Cash System. The article proposes that it is hoped that a new type of electronic payment system can be created. This system "is based on cryptographic principles rather than on credit, so that any parties that reach an agreement can directly make payments and thus do not need third-party intermediary participation." The paper gave birth to Bitcoin, which marked a major step forward in the human society's monetary system. Bitcoin adopted the design idea of open distributed ledgers, and it really got rid of the constraints of third-party institutions. Then Bitcoin entered a period of rapid development.

On January 3, 2009, the first block of the blockchain was born. This block is also called "Creation Block".

On January 12, 2009, Nakamoto sent 10 bitcoins to the cryptographer Harfini;

In July 2010, the establishment of the Bitcoin exchange Mt.Gox, Bitcoin's value was recognized worldwide.

In the following years, due to the huge resource consumption caused by Bitcoin's mining mechanism, the anonymity of Bitcoin poses a challenge to traditional financial supervision, which has caused Bitcoin prices to rise and fall.

Jump from Bitcoin to Blockchain +

The birth of the blockchain marks the beginning of the construction of a truly trustworthy Internet. By combing the rise and development of the blockchain, we can see that the blockchain attracts people's attention because it can establish reliable trust between the point-to-point in the network, which makes the value transfer process eliminate the interference of the intermediary, and both discloses information and protects privacy. Both the joint decision-making and the protection of individual rights and interests, this mechanism improves the efficiency of value interaction and reduces costs.

Blockchain technology has been deployed and applied throughout the world. Developed countries such as the US, UK, Japan, Germany, Canada, and Australia have realized that there is a huge application prospect for blockchain technology in the optimization of public services and social mechanisms. Blockchain development path.

There are currently two major application trends:

From the perspective of public services, blockchain technology is exploring

applications in areas such as public administration, social security, intellectual property management and protection, and land ownership management. Relevant practices have shown that this technology can help increase public participation, reduce social operating costs, improve the quality and efficiency of social management, and have an important role in promoting the improvement of social management and governance.

From an economic and social point of view, the blockchain economy has sprouted. Many blockchain-based solutions can improve existing business rules, build new types of industry collaboration models, and increase the efficiency of collaborative circulation. Both central banks and major commercial banks, as well as the United Nations, the International Monetary Fund, and many national government research institutions, have devoted great attention to "blockchain+" investment.

Blockchain can provide systematic support for economic and social transformation and upgrading. The significant advantages of Blockchain+ are the optimization of business processes, the reduction of operating costs, and the enhancement of collaborative efficiency. This advantage has been preliminarily reflected in various fields such as financial services, supply chain management, intellectual property, smart manufacturing, social welfare, education and employment.

1.2.2 Blockchain Design Ideas

The foundation of value interaction is the establishment of mutual trust. The revolution of blockchain technology lies in the fact that it has realized a brand-new

way of trust. Through the design innovation at the technical level, the trust relationship between people can be transformed into the trust of people and technology, and even the automation of the process. By implementing certain aspects, commercial activities can be realized at a lower cost.

Economic design ideas

From a economic point of view, this new paradigm of value interaction created by blockchains is based on "weakly centralized," but this does not mean that the "centers" in the traditional society completely disappear and that there will be a large number of blockchains in the future. The "multi-center" system is dominated by alliance chain, private chain, or mixed chain. Blockchain will further improve the "central" operating efficiency and reduce a considerable part of its costs.

Technical level design ideas

From a technical point of view, we believe that blockchain is a technology system that is maintained by multiple parties, stores data in a blockchain structure, uses cryptography to ensure transmission and access security, and can implement consistent data storage, irreversibility, and non-repudiation. . This kind of technology has brought unlimited space for the world to think about. The global attention to the blockchain continues to heat up. The major economies in the world have begun to study blockchain technology and development trends from the national strategic level.

1.2.3 Blockchain Features

Decentralization: Due to the use of distributed accounting and storage, there is no centralized hardware or management organization. The rights and obligations of any node are equal. The data blocks in the system are maintained by the nodes with maintenance functions in the entire system. .

Openness: The system is open. Except that the private information of the parties to the transaction is encrypted, the data of the blockchain is open to everyone. Anybody can query the blockchain data and develop related applications through the open interface, so the whole system Information is highly transparent.

Autonomy: The blockchain uses consensus-based specifications and protocols (such as a set of open and transparent algorithms) to enable all nodes in the entire system to exchange data freely and securely in a trusted environment, making the trust of "people" changed. Become a trust in the machine, any human intervention does not work.

Cannot be tampered with: once the information is verified and added to the blockchain, it will be stored permanently. Unless more than 51% of the nodes in the system can be controlled at the same time, the modification of the database on a single node is invalid, so the blockchain The data stability and reliability are extremely high.

Anonymity: Since exchanges between nodes follow a fixed algorithm, their

data interaction is not trustful (the program rules in the blockchain will automatically determine whether the activity is valid), so the counterparty does not need to make the other party produce its own identity. Trust is very helpful to the accumulation of credit.

1.2.4 Core Technology of Blockchain

Blockchain technology is not a single-item technology, but a comprehensive technology system that integrates multiple research results. We believe that there are three indispensable core technologies: consensus mechanism, cryptographic principles, and distributed data storage.

Consensus mechanism

The so-called consensus refers to the process in which nodes participating in multiple parties agree on certain data, actions or processes through interactions between multiple nodes under preset rules. The consensus mechanism refers to the algorithms, protocols, and rules that define the consensus process. The consensus mechanism of the blockchain has the characteristics of "majority to the minority" and "equality for all". The "majority to the minority" does not exactly mean the number of nodes, but also the computing power, the number of shares, or other computers. Feature amount. “Everyone is equal” means that when a node satisfies a condition, all nodes have the right to give priority to the consensus result, be directly recognized by other nodes, and finally may become the final consensus result.

The principle of cryptography

In the blockchain, the dissemination of information is based on asymmetric digital encryption technology such as public key and private key to achieve mutual trust between the parties. In the specific implementation process, after one key pair information in the public and private key pair is encrypted, only the other key can be used to unlock the process. And after one of the keys is disclosed (that is, the public key is public), another undisclosed key (that is, the private key) cannot be calculated based on the public key.

Distributed storage

The distributed storage in the blockchain is that the participating nodes have their own independent and complete data storage. Different from traditional distributed storage, the uniqueness of distributed storage in blockchain is mainly reflected in two aspects: First, each node of the blockchain stores complete data in a block chain structure, and traditional distributed storage. Generally, the data is divided into multiple copies according to certain rules for storage. The second is that the storage of each node of the blockchain is independent and equal in status, and the consensus mechanism is used to ensure the consistency of storage. However, traditional distributed storage generally synchronizes data with other backup nodes through the central node. Data nodes can be different physical machines, or they can be different instances in the cloud.

1.3 The Future of Value Internet of Things

The traditional Internet of Things (IoT) is a network that enables all common objects that can perform independent functions to achieve interoperability. It connects sensors, controllers, and objective entities through network technologies to achieve intelligent management and control. For example, information sensing devices such as radio frequency identification (RFID), infrared sensors, global positioning systems, laser scanners, etc., connect any item to the Internet in accordance with the agreed protocol, and perform information exchange and communication to realize intelligent identification and positioning. , tracking, monitoring and management. As an extension of the Internet, the Internet of Things (IoT) further promotes the connection between machines and machines, people and machines, and realizes the flow of data throughout the entire life cycle of the information world.

With the continuous advancement of technology, the development and application of Internet of Things technology has achieved remarkable results in recent years. At present, billions of sensors and intelligent controllers have been put into use around the world. This number is expected to increase in the next few years. It will also grow exponentially. However, the Internet of Things technology is also faced with many problems and challenges, such as the lack of tag data acquisition, the high risk of centralized data storage, and the high cost of security in Internet of Things applications in the financial sector. These issues may become the Internet of Things. Great obstacles to future development and application. The value Internet of Things led by RFID technology and blockchain technology can provide solutions

to these problems.

The technology realization of value Internet of Things is to connect the physical tags such as item tags, event tags, and human body tags in the real world to the virtual world of the Internet through a low-level hardware platform built with RFID chips as the core, and to combine blockchains. Technology is the link that conveys value and constructs trust, realizing the interconnection of all things.

The transition from the information Internet and traditional Internet of Things to the value-based internet of things based on RFID technology and blockchain technology may be far faster than the current people's expectations. When the value of the Internet of things truly realizes interconnection and interoperability, RFID technology And blockchain technology will get more play.

Part Ⅱ the Global Value Chain

2.1 Global Value Chain Interpretation

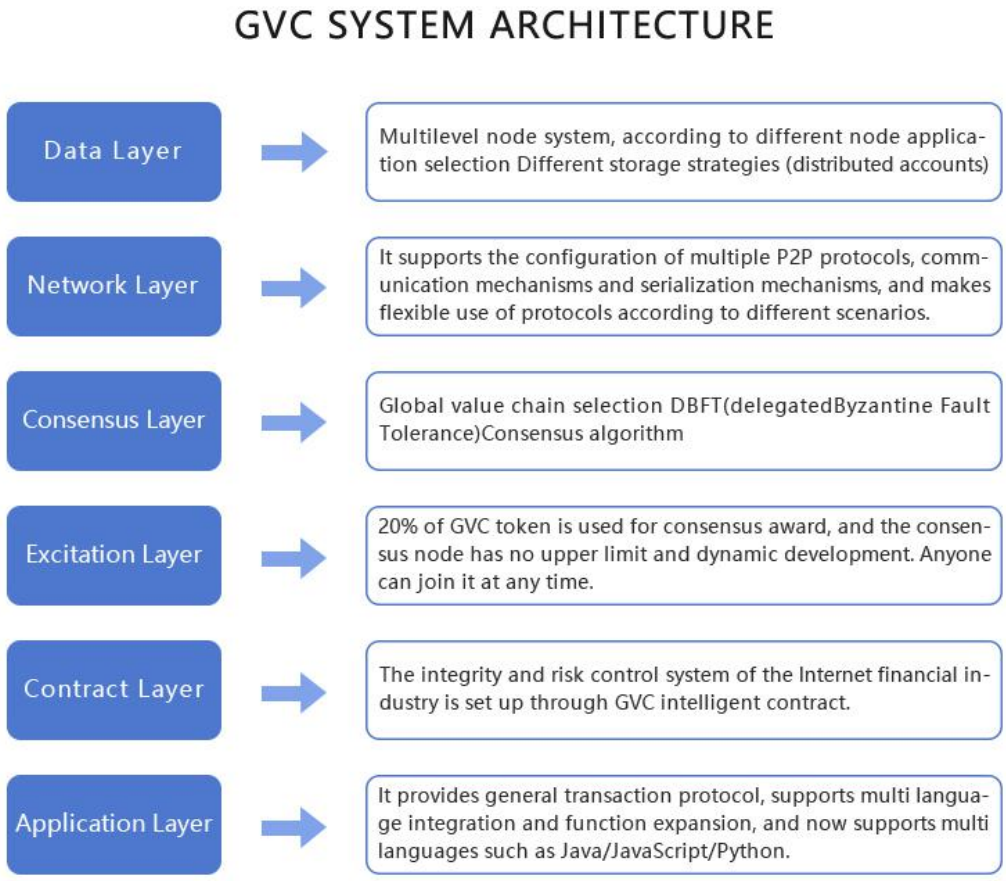
The concept of the value chain was first proposed by Michael Porter in "Competitive Advantage" (1985). Porter believes, "Every business is an aggregation of activities in the process of designing, producing, selling, sending, and supporting its products. All these activities can be expressed in a value chain."

The global value chain, English Global Value Chain, or GVC, aims to create a new value Internet of Things ecosystem that is interconnected with each other, assist each other, and develop together. It is a value-based IoT underlying public chain based on blockchain technology.

2.2 Technology Application

2.2.1 Safe System Structure

There are six layers of Global Value Chain (GVC) architecture: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer.



Data layer

Based on the blockchain-based high-redundancy storage mechanism, blockchain storage has a certain impact on the scalability and performance of the blockchain. The global value chain framework is designed with a multi-level node system, and different choices according to different node applications. Storage strategy (distributed accounting).

Accounting node: The core role of GVC, entrusted by GVC holders to participate in

the consensus mechanism and manufacturing block.

All nodes: Responsible for the preservation of complete data, but do not participate in consensus, listen and relay the transaction. Ordinary users access directly through the interface or the user side without saving data. The advantage of a multi-level node system is that it does not want nodes to participate in billing (mining), store complete data, and relay transactions. Because not all nodes have common aspirations and want to save complete data, GVC design allows the entire system to have a clear division of roles. Professional nodes do professional things, which saves energy and improves overall system efficiency.

Network layer

The P2P protocol supports the data transmission and signaling exchange of each node in the blockchain network. It is an important communication guarantee achieved by the data distribution or consensus mechanism. The GVC system design supports multiple P2P protocols, communication mechanisms, and serialization mechanisms. The configuration requires flexible protocol usage depending on the scenario. In terms of communication security, it is possible to flexibly support secure communication protocols such as HTTPS, TLS, and WSS (Secure Web Sockets). On the need to establish a platform to apply external service interfaces, authentication extensions that support OAuth can be extended.

Consensus layer

The global value chain selects the dBFT (delegatedByzantine Fault Tolerance) consensus algorithm, which is a Byzantine fault tolerance consensus algorithm

based on voter voting. It has the characteristics of high performance and high consistency. It is suitable for financial payments, and the digitized transaction data is frequently generated. High-level real-time billing requirements for weak upper-layer applications. Traditional blockchains need to achieve a certain number of block confirmations due to the setting of accounting rules, so that the confirmation of the chain can be completed at a certain probability. That is to say, when a block is added to a block, it can guarantee 100% certain future. It is this chain that has always been slightly overturned. Basically it takes up to 99.999999% of confirmed transactions in 6 blocks. The finality of the transaction under this model is relatively weak, and it is not suitable for the top-level applications of digital payment such as digital asset trading platforms. The dBFT consensus algorithm can maintain block consistency. This consensus algorithm selects account holders according to the ratio of equity occupation, and the bookkeepers then reach consensus through the Byzantine fault tolerance algorithm. With certain endorsements and trust, it is unlikely that more than one-third of the billing nodes will colluding and doing evil. Even if this happens, cryptographic evidence can be used to run post-mortem evidence for accountability.

The advantages of this approach are:

(1) Specialized bookkeepers;

(2) Can tolerate any type of error;

(3) The bookkeeping is done by many people. Each block has its finality and will not be forked;

(4) The reliability of the algorithm has strict mathematical proofs; The core point of the dBFT mechanism is to ensure the finality of the system to the utmost, without bifurcation, which is very suitable for the digital payment application scenario.

Excitation layer

20% of the tokens of the global value chain are used for consensus rewards. Because of the unique consensus mechanism of GVC, the performance is not affected by the number of nodes. Therefore, the GVC consensus node does not have an upper limit, and is dynamic and can be changed at any time. Join to earn rewards.

Contract layer

For each smart contract, it runs full life cycle management as a financial asset on the chain, complete and controllable process management for the submission, deployment, use, and cancellation of smart contracts, and integrates the various rights management mechanisms for smart contract operations. Mechanisms for comprehensive security management. The integrity and risk control systems of the Internet finance industry have been set up through GVC smart contracts, including P2P, crowdfunding, private equity, and internet financial affiliate products. For example, an inbound contract, signed by both parties through a smart blockchain contract, will be sold on an agreed-upon basis within the time limit specified in the future.

Application layer

The application layer will provide common transaction protocols, support for multiple query integration, and feature extensions. Currently, it supports multiple languages such as Java, JavaScript, and Python. At present, it has developed and implemented a general financial integrity agreement. Actually, this agreement is not just the use of integrity in Internet finance. protocol.

2.3 Core Technology

2.3.1 POW+POS

The global value chain refers to the problems in the previous stage of the development of the blockchain, like the storage problems caused by the BTC's pow technology, adopting the new hybrid mechanism pow+pos technology, and all coin holders can participate in the community's important decisions through the PoS mining mechanism. , including updates and upgrades of the agreement. More advanced is that GVC provides a smooth execution method. Once the vote is passed, all decisions will be recorded on the blockchain and enforced, thus avoiding the miners, mining pools, exchanges, wallet service providers. Collaboration problems. The existence of the PoW mechanism is to prevent the early investors from occupying too much of the revenue in the PoS distribution mechanism. At the same time, the PoW has been previously proved to be the most effective in securing blockchain-based system security mechanisms. Although it inevitably consumes a part of energy, we consider it worthwhile to consider the system that effectively guarantees the safety of the system, and the mining process

of PoW + PoS is organically combined to ensure the safety of the system. Sex.

Start mining with this traditional PoW approach and compete against each other to solve the secret puzzle. According to this implementation, the dug-out blocks do not contain any transactions (they are more like templates), so the winning block will only include one header and the miner's bonus address. At this point, the system will switch to PoS. Based on this header information, a set of random validators is selected to sign the new block. The greater the probability that a validator holding more coins is selected. Once these selected validators complete the signature of the block, the template becomes a complete block. If these selected validators are not available to sign the block, they will be selected to sign the next block and then a new set of validator signatures will be selected until the block gets the correct number of signatures. The fee will be allocated to the miners and the validators who sign the block.

For PoW, qualified blocks can be expressed as: F(Nonce) < Target

Where Nonce is a random element, Target is the quantification of a qualified block, and the Target of each accounting node is the same. In addition, the successful use of PoW also requires the following two agreements:

1, Best chain principle: The longest chain is considered the correct chain.

2. Incentive principle: There are incentive benefits for finding qualified blocks.

Article 1 is that the mandatory rules must be complied with. The common goal is to find consistency books, and the longest chain represents the largest amount of work. Without this agreement, everyone will only build their own blockchain and

cannot achieve Consistent. Article 2 is workload incentives. Since there are costs for bookkeeping, then only the benefits can drive everyone to keep accounts. Participating in the book-building block becomes an investment behavior, and the cost and revenue risks form a game under the first constraint. , Drive all nodes to build blocks honestly according to the agreed rules, and eventually reach Nash equilibrium.

For PoS, qualified blocks can be expressed as: F(Timestamp) < Target * Balance

The above PoS method is the current PoS mechanism adopted by nxt and Blackcoin. The most streamlined version of the PoS mechanism can easily lead to the problem of wealth centralization and at the same time it has a major impact on overall system security. Therefore, we must consider Stake(Balance) and add another variable to avoid the centralization and security problems caused by the simple reference to Balnace. Compared to PoW, the search space on the left of the formula changes from Nonce to Timestamp, the Nonce range is infinite, and the Timestamp is extremely limited. The block time of a qualified block must be within the specified range of the previous block time. Blocks that are too early or too advanced will not be accepted by other nodes. The target value on the right side of the formula introduces a multiplicative factor balance. The larger the visible balance, the larger the Target * Balance, and the easier it is to find a block. Because of the limited Timestamp, the success rate of PoS casting blocks is mainly related to Balance (Stake).

The PoS mechanism of GVC will learn from the existing PoS mechanism. On the premise of ensuring the security of the system, it refers to the efficiency of the PoS and focuses on the security of the digital currency when users use the PoS mechanism.

2.3.2 Zero Knowledge Proof

Zero-knowledge proof (referred to as "zk-SNARK") is the core technology that implements the anonymous nature of Zcash. The definition of "zero-knowledge proof" is that the prover can convince the verifier that a certain assertion is correct without providing any useful information to the verifier.

Considering GVC's massive volume of data interaction, we adopt a security scheme that is based on the difficulty of calculating the discrete logarithm. We can do pre-computation to reduce the amount of real-time computation and reduce the amount of data that needs to be transmitted. In order to generate a key pair, the parameters of the system need to be selected first: the prime number p and the prime number q, q is the prime factor of p - 1 . $p \approx 21024$, $q > 2160$, element g is a q-order element, $1 \leq g \leq p - 1$. Let a be the generator of GF(p), then get $g = a(p - 1) / q \bmod q$. The trusted third party T distributes the system parameters (p, q, g) and verification functions (ie, T's public key) to each user, and uses this to verify the signature of the T-to-message. For each user given a unique identity I, User A selects the secret key s, $0 \leq s \leq q - 1$, and calculates $v = g{-}s \bmod p$; A gives IA and v reliably to T, and from T gets a certificate, CA = (IA, v, ST (IA, v)).

The agreement is as follows:

(1) Select the random number r, $1 \leq r \leq q - 1$, calculate $x = g^r \bmod p$, this is a preprocessing step, which can be completed before B appears;

(2) A sends (CA, x) to B;

(3)B solves ST (IA, v) with T's public key, realizes the authentication of A's identity IA and public key v, and transmits a random number e between 0 and 2 t - 1 to A;

(4) A verifies that $1 \leq e \leq 2t$, calculates $y = (se + r) \bmod q$, and sends y to B;

(5)B verifies $x = g^y v^e \bmod p$. If this equation holds, then the identity of A is valid.

The security is based on the parameter t, which is chosen to be large enough so that the probability 2^{-t} of correct guessing e is large enough. It is recommended that t be 72 bits, p approximately 512 bits, and q 140 bits.

This protocol is a zero-knowledge proof of s, and no useful information about s is exposed during the certification process.

GVC will draw on Zcash's zero-knowledge proof technology. It can not only realize two-way encryption in the process of asset transfer, but also can be applied to many other areas where transaction privacy requirements are extremely high. GVC integrates the instant messaging function on the client. It not only can use the dark address to realize cross-platform transfer of tokens, but also can use zero-knowledge proof mechanism to achieve high-private communication in normal peer-to-peer (P2P) communication, and can also leapfrog. The platform implements encrypted communication such as from the Hcash client to the Byteball client.

2.3.3 Post-quantum cryptography

In the current blockchain system represented by Bitcoin, SHA-256 hash calculation and ECDSA elliptic curve cryptography constitute the most basic security guarantee for the Bitcoin system, but as quantum computer technology continues to make breakthroughs, especially The Xiao algorithm is the representative of the classical quantum algorithm. The related operation can theoretically achieve the transition from the exponential level to the polynomial level. These problems that are "difficult" for classical computers will surely be applied in the foreseeable future. Quantum computer cracked.

Post-quantum cryptography, also known as quantum-resistant cryptography, is a cryptosystem that is believed to be resistant to quantum computer attacks. The development of such encryption technology takes a traditional approach, that is, based on the difficult problems in a specific mathematics field, it is applied to network communications through research and development algorithms to achieve the protection of data security. The use of post-quantum cryptography does not depend on any quantum-theoretic phenomenon, but its computational security is believed to be able to withstand any form of quantum attacks currently known. In 1997, an IBM researcher proposed an encryption scheme called Learning With Errors (LWE), which means that learning is accompanied by errors. Because it takes a long time to find the nearest common cell, it can resist attacks from quantum computers.

Ring-LWE Based Public Key Encryption Scheme

Related parameter selection and operation rules

The main parameters in the scheme are n, p, q.

n: Determines the maximum number of polynomials in the encryption scheme. Under the standard of guaranteeing the calculation efficiency and safety, the larger the value of n is, the better, it should be 2k.

q: Large modulus, usually a positive integer, the size of q is related to the specific instance. The value of q should be large enough to guarantee high enough security. However, the larger the q value, the more system resources will be used and the greater the amount of integer calculation.

p: Small modulus, usually a small positive integer.

Let R = Z

q[x] / (xn + 1) for the two polynomials f and g in the ring, expressed as f(x) = f0 + f1(x) +... + fn-1xn-1,g(x } = g0 + g1(x) + ... + fn-1xn-1,k ∈ R, The following operations are defined: k · f(x) = kf0 + kf1x+ ...kfn-1xn-1

Key generation

In this scheme, the encryption public key is h(x), and the decryption private key is f(x) and fp(x). The selection method is as follows to select the polynomials f(x), g(x) to satisfy:

f(x) ·g(x) =0modq.

f(x) · fq(x) = 1 modq.

h(x) = fq(x) + 1.

The public key is (h(x), g(x)) and the private key is (f(x), fp(x)).

Encryption process

In this scheme, the random error polynomial $e(x) \in \Psi\alpha$ is referenced when encrypting, and $\Psi\alpha$ is a certain Gaussian distribution with parameter α. The plaintext is converted into a polynomial m(x), and the ciphertext is calculated as: c(x) = h(x)·m(x) + g(x) ·e(x).

Decryption process

The received ciphertext is c(x). The steps to decrypt the ciphertext using the private keys f(x) and fp(x) are as follows:

α(x) = f(x) · c(x) = f(x) · h(x) · m(x) + f(x) · g(x) · e(x) = [f(x) Fq(x) + f(x)]·m(x)+f(x) ·g(x) ·e(x) modq = f(x) ·m(x)(1)

fp(x) ·a(x) = fp(x) ·f(x) ·m(x) modp= m(x) (2)

The decryption failure may occur during the decryption of steps (1) and (2), ie when the coefficient of step (1) is not within the interval (-q2, q 2) or the coefficient of step (2) When the interval is not between (-p2, p2), the decryption failure occurs, but as long as the appropriate parameters are selected, the possibility of decryption failure is still very small, and a method similar to NTRU to avoid decryption failure can also be used. Reduce the probability of decryption failure.

GVC will develop a Ring-LWE key exchange protocol that works with OpenSSL to implement the security issues of the post-quantum era blockchain.

2.3.4 IPFS Interplanetary File System

IPFS is a network transport protocol that creates persistent and distributed storage and shared files. It is an addressable peer hypermedia distribution protocol. The super contract books based on the TCC underlying code mechanism will have the same file management model in the future. Substantial subversion of cloud storage and IPFS connected computer devices. In fact, IPFS is a single Bittorrent user group that mutually forwards Git targets. IPFS has the qualities of becoming an Internet subsystem, and can be fully configured or even replaced by reasonable configuration, and all computing devices with the same file system can be connected together. The principle is to use content-based addresses instead of domain name-based addresses. That is, the content that the user is looking for is not an address but stored somewhere. It does not need to verify the identity of the sender, but only needs to verify the hash value of the content. This approach can be faster, safer, more robust, and more durable.

IPFS replaces traditional domain name-based addressing with content-based addressing. Users do not need to care about the location of the server, and do not consider the file storage name and path. We put a file in the IPFS node and we will get the unique cryptographic hash calculated based on its content. The hash value directly reflects the content of the file. When IPFS asks for a file hash, it uses a distributed hash table to find the node where the file is located, retrieves the file, and validates the file data.

2.3.5 DAG

The DAG technology itself is not based on blocks, so it is not limited by the block confirmation time (for example, Bitcoin's block confirmation time is 10 minutes and Ethereum's confirmation time is about 15 seconds). Because GVC needs to consider the interaction with the blockchain system based on DAG technology during system design, it will draw on the features and advantages of DAG. The confirmation time of the transaction in the GVC system is almost instantaneous. At the same time, because DAGs are not based on blocks, there is no limit to the block size. Theoretically, the volume of transactions that can be accommodated per unit time is very large (HTPS, Hyper Transaction Per Second). At the same time, GVC needs to consider the interaction with the block-based blockchain system. So GVC can realize mass transactions per unit time under a limited block size.

2.4 Global Value Chain Ecosphere

2.4.1 Consumption Payment

he global value chain (GVC) will serve as a circulation of consumption for payment, fully utilize the characteristics of decentralization and intangible modification of blockchains, and distributes consumer cooperation services in a number of countries around the world, involving food, clothing, shelter, Use, line and other fields, on the one hand improve the mall's efficiency and service levels, on the other hand can better protect the rights and interests of consumers.

In China, the Global Value Chain (GVC) team has established a cooperative relationship with Hua Mall, and GVC will access the circulation on schedule. Hua Mall is an online and offline large-scale integrated B2B2C e-commerce shopping mall, adhering to the business philosophy of consumption sharing and win-win cooperation. A complete consumer system builds credit value-added systems, big data systems, and near-perfect user experiences to provide better and better

services to consumers and businesses. After years of operation and building, the number of registered members of Hua Mall has exceeded 120,000, and the daily volume of online transactions has exceeded 1,000, and the monthly transaction volume has exceeded 5 million. By then, GVC users in China will be able to use GVC to purchase their favorite products in China Mall, realizing consumer payment circulation.

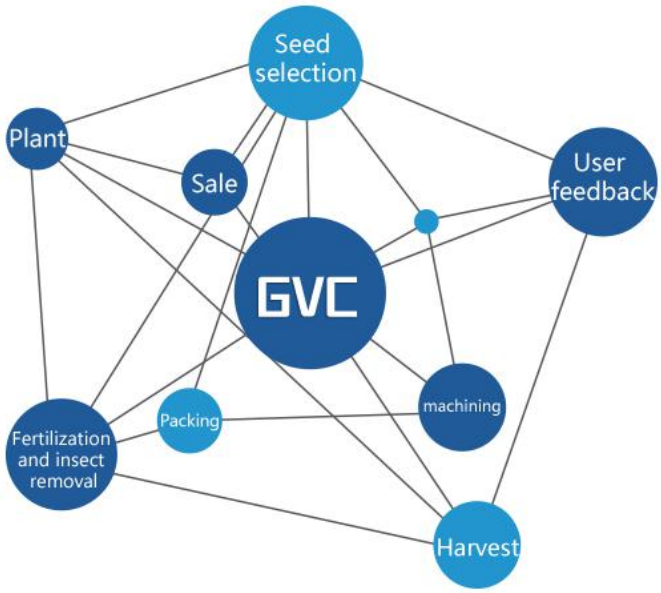
The Global Value Chain (GVC) will also integrate the global cooperation malls, organically integrate cross-border e-commerce, local e-commerce, and physical malls so that all consumers can really build a product without leaving home and buying products from all over the world. The whole consumer pays for the value of the ecosystem.

2.4.2 Anti-Counterfeit Tracing and Enhancing Efficiency

Counterfeiting has always been a major problem for social development. With the development of society, this contradiction has become increasingly prominent. Solving this problem has become an urgent task. Take food as an example. Although there are green food labels, there are too many questions about the credibility of data in the middle link because human factors are involved in the entire supply chain. This has a big doubt on the credibility of the society and the company. influences. Whether food is green and pollution-free or whether high-end arts/luxury goods are fakes and so on remains a series of issues. Blockchain technology relies on its data non-deterrence, transaction traceability, and timestamp existence proof mechanism, which can well solve the disputes arising from the tampering of data among parties in the supply chain system, and achieve effective accountability and products. Security.

Cambodia is a big country in agriculture, with rich varieties of rice and other agricultural products. The global value chain (GVC) has introduced blockchain technology to trace the origin of agricultural product supply chains, and has selected agricultural products — planting — fertilizing and removing pests — -

Harvesting - Processing - Packaging - Sales - User feedback, etc. Each link of the entire chain is written to the blockchain, using the traceability of the blockchain and the inability to modify the source Every link is strictly controlled, and the elimination of counterfeit and shoddy products from the source to the market is introduced. After introducing GVC, some unnecessary links can be omitted, and the efficiency is improved to some extent. All users can query the chain at any time during the entire process. Source selection, planting, processing, packaging, sales, user feedback, etc., increase the user's trust and have important significance for the development of local agricultural products.



2.4.3 Financial Payment

The core of finance is the establishment and transmission of credit. The blockchain is naturally adaptable to a variety of financial scenarios because of its characteristics of being irrevocable, safe, transparent, decentralized, or polycentric. Most blockchain alliances at home and abroad have focused on the financial sector. For example, the blockchain alliance R3, which consists of 42 international banks, is committed to using blockchain technology to build a flat global integrated settlement based on mutual trust. System to increase efficiency and reduce costs. In addition, McKinsey estimates that blockchain technology can reduce the cost of cross-border transactions from $26 to $15. Goldman Sachs also pointed out in a report that blockchain technology will save the capital market $6 billion in annual costs.

Cross-border payments

The two biggest pain points in the telegraphic payment industry in existing international trade are in withdrawal:

The first type is that, under the cash on delivery model, exporters may lose money and goods. Under this settlement method, if the exporter fails to pick the importer with a high credit rating and provides the goods transport document to the importer, he loses control over the goods. In addition, the exporter has not received the payment in advance, once the importer is encountered. If the goods are received but no payment is made, the exporter will face the dilemma of

financial and material losses. Under the traditional payment model, since there is no guarantee that the importer can actually make the payment, the exporter will bear a great deal of risk once the cash on delivery model is adopted.

Second, in the prepayment mode, the importer did not receive the payment. In this settlement mode, importers are exposed to relatively large risks. After the importer pays the purchase price, he or she will worry that the exporter will not deliver the goods or not deliver the goods according to the contract. The exporter is the beneficiary and can obtain funds in advance for safe production. Under the traditional payment model, once the importer wired part of the funds in advance, the exporter could not be constrained, and therefore faced with the risk of payment but not receiving the goods.

Since the telegraphic transfer model needs to be based on commercial credit between the two parties, there is always a contradiction between the buyers and the sellers in the choice of payment methods in international trade. The core focus is on mutual trust between traders and trade. The problem of cash flow during the process. In order to solve the increasingly frequent international trade exchanges, we must find a proper and trustworthy mechanism to complete the entire payment and exchange process.

Blockchain is an integrated innovation of information technologies such as distributed data storage, peer-to-peer transmission, trust consensus algorithms, and encryption algorithms in the Internet era. It has features such as pan-centralization, trust consensus, non-destructive information, and openness,

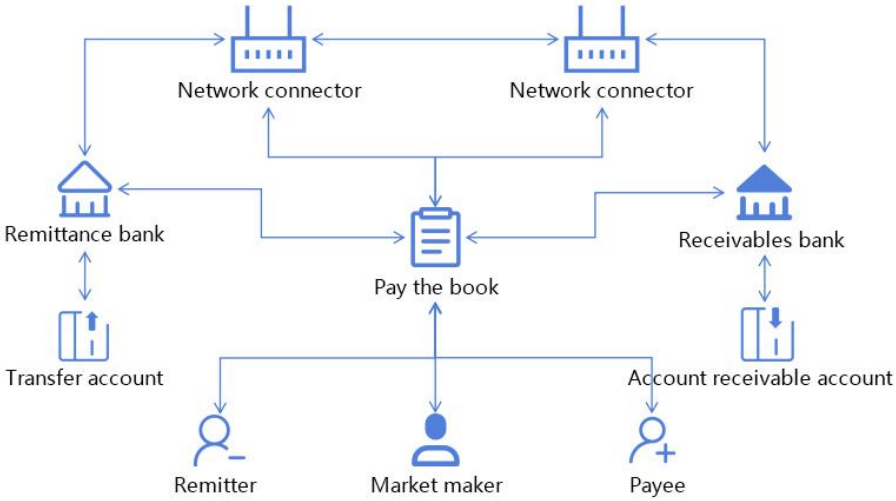
and is suitable for both parties. Need a highly trusted business scenario. The use of new blockchain technology to build a set of cross-border payment and settlement systems that are mutually point-of-view and mutually trustable can further increase the efficiency of cross-border payment, increase the safety and reliability of cross-border payments, and greatly promote the development of international trade.

The global value chain is used in cross-border payment services. Using blockchain networks, traditional financial institutions, foreign exchange market makers, liquidity providers, etc. are added to the payment network to build a payment gateway. Through the payment gateway, the flow of digital assets in the blockchain can be connected with the legal currency in reality, and the legal currency can be converted into GVC, facilitating subsequent payment and transfer. Through the network linker in the blockchain payment network, traditional market makers, export banks, and import banks can be connected, eliminating intermediate transaction links and achieving point-to-point fast and low-cost payment.

According to the current traditional network payment architecture and in-depth analysis of the cross-border payment transaction process, this article combines the characteristics of blockchain technology to build a blockchain-based GVC cross-border payment solution.

GVC payment architecture diagram

GVC payment architecture diagram



Blockchain-based GVC cross-border payment solutions include two major roles and four modules. The two major roles are various agencies and customers involved in blockchain payments. Are as follows:

The first role is the gateway, which can be a bank, a market maker, a liquidity provider, etc. The main role of the gateway is to allow the legal fiance in reality to enter the blockchain payment network.

The second role is the customer, which can be a variety of international trade

customers. The customer is the relevant party involved in the blockchain payment transaction and participates in confirming the transaction information. In the course of a transaction, once either party has not confirmed the transaction, the transaction cannot be officially put into effect.Through this common verification, the risk of information opacity is greatly avoided, and the risk of cross-border payment in international trade is reduced.

The four major functional modules in GVC cross-border payment are the core business logic modules for realizing cross-border payment. Are as follows:

The first functional module is a network connector. It is a tool to help various agencies as gateways and access blockchain payment networks. The network connector is a "plug-and-play" function module that can be integrated with existing international payment systems so that banks can handle cross-border payment services through blockchain payments. This module connects remittance bank and receiving bank to exchange personal information, expenses, delivery details, payment details, etc. After the system confirms the transaction information of both parties, the module connects the blockchain to pay the book of accounts for settlement, and notifies all parties to confirm the transaction.

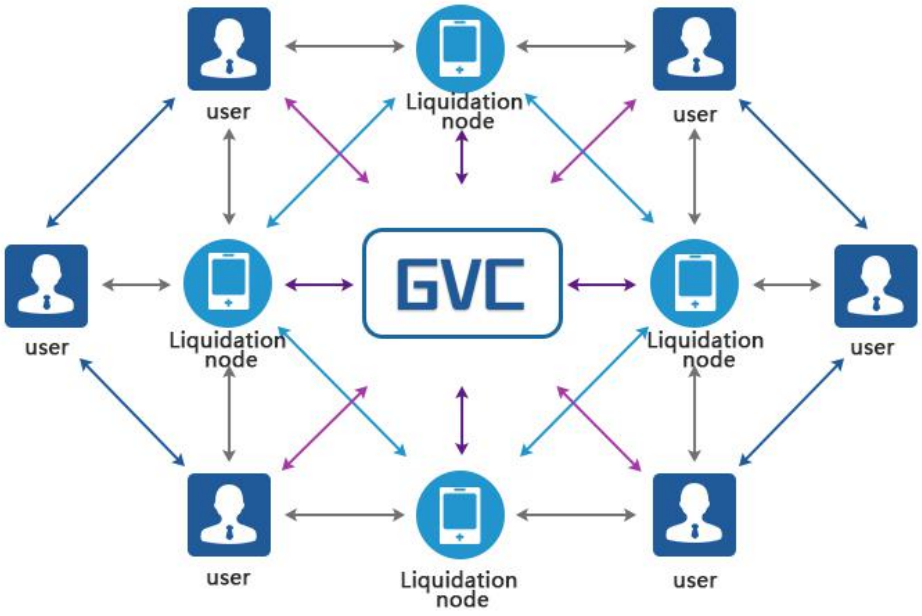
The second functional module is the blockchain payment book. Banks, market makers, etc. are used as nodes to access blockchains to pay for books.

The third functional module is the market maker client. The market maker submitted the foreign exchange price to the blockchain payment account. The bank's internal foreign exchange trading platform can also be integrated into the

blockchain payment network through this module, thereby realizing market maker functionality.

The fourth functional module is the trading client. The client can directly operate the blockchain payment through the client, and can also initiate payment through a financial institution like the traditional mode.

Clearing/Settlement of Transactions



The process of transaction clearing/settling is also the process of separate accounting between the two parties. In the traditional transaction mode, the

accounting process is performed separately by the parties. Not only does it cost a lot of manpower and material resources, but it is also prone to inconsistent account reconciliation, affecting settlement. effectiveness. Through the GVC blockchain system, both parties or parties to the transaction can share a set of trusted and mutually-recognized ledgers. All transaction clearing and settlement records are all available in the chain, which is safe and transparent, cannot be tampered with, and can be traced, greatly improving the accuracy of reconciliation. Degree and efficiency. Through the implementation of smart contracts, it is also possible to achieve automatic settlement of transactions, greatly reducing the cost and error rate of the reconciliation personnel, especially in the context of cross-border payment.

Insurance against fraud

The global value chain GVC uses consensus mechanisms, anti-tampering mechanisms and traceability mechanisms to provide effective evidence support in insurance compensation and recovery. Take automobile insurance claims as an example, it usually includes owners, 4S shops or repair shops, insurance companies, and traffic control departments. Cheats and other claims fraud problems often occur. Relying on blockchain technology and vehicle networking technology, the corresponding sensor recording equipment is installed on the vehicle to ensure that the information is true, accurate and irrevocable. When the vehicle is out of danger, the vehicle accident data is submitted to the application blockchain technology in real time or quasi-real time. The "accident authentication platform"

system, traffic police decision data, sensor logger data, maintenance plant data, etc. are all synchronized in real time, fundamentally solving the auto insurance claims fraud problem, and at the same time improving the efficiency and accuracy of insurance claims cases.

2.4.4 Tourism circulation

Tourism is one of the important industries for social development. With the growth of the economy and the improvement of people's living standards, tourism has gradually developed into one of the pillar industries for social development. But at the same time, it also exposes the length of the industry chain, and the transaction process involves Many intermediate links and other issues.

Cambodia has a wealth of tourism resources. The global value chain GVC is used in the tourism industry. It can fully exploit the advantages of multi-blockchain participation, openness, transparency, consensus trust, traceability of traceability, indiscernibility, privacy protection, etc., and build a chain tourism ecology. , Combining different application scenarios of different tourism participants, provide standardized, intelligent, and big data support services to provide support for real-time monitoring, daily management, and key decision-making of tourism management departments; and achieve efficient management and intelligent services for tourism service providers. , precision marketing and other business promotion; for tourism consumers bring convenient, efficient, credible, favorable travel experience.

Global value chain GVC accesses the tourism industry and will build a brand new decentralized, safe and trusted tourism ecosystem. It will also build tourism trust communities, purchase travel insurance, identity certificates, travel reviews, hotels and flight reservations, etc. Circle, further promote and improve the construction of the ecological circle.

2.5 Allocation mechanism

2.5.1 About Global Value Chains

The global value chain is a full-code open-source encrypted digital asset based on BTC's underlying technology. It is a public chain of the bottom chain of the

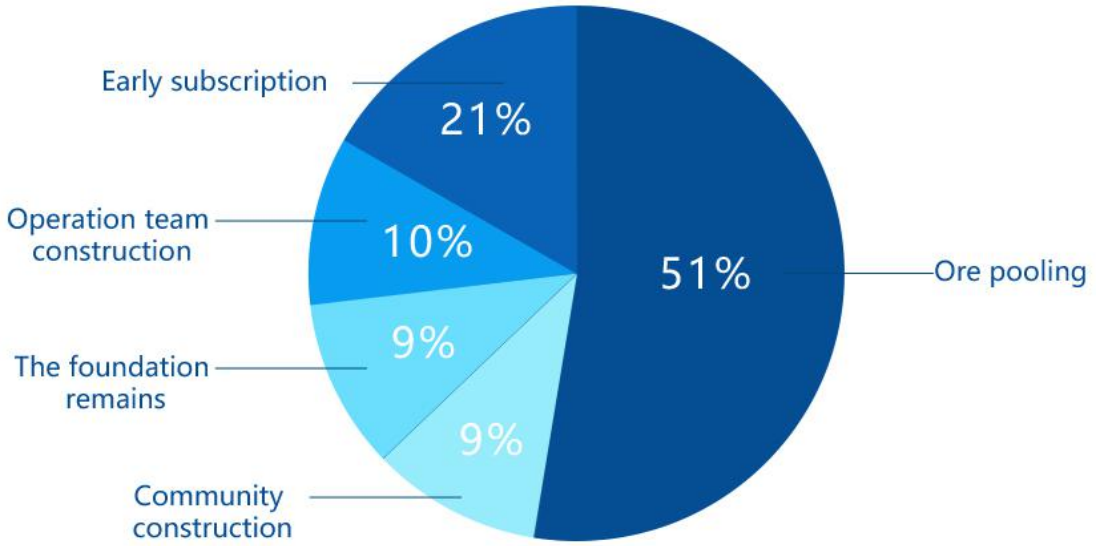
blockchain. It also provides cloud mining machines, mining software, hardware, and wallets. The total value chain of the global value chain is 100 million pieces, and its security is guaranteed by the Elliptic Curve Digital Signature Algorithm (ECDSA).

2.5.2 Vision of Global Value Chain

The global value chain is determined to build the bottom public chain of value Internet of Things applications. It hopes to use blockchain + Internet of Things technology to solve the difficulties in the development of the Internet of Things and create a new value of the Internet of Things ecosystem. At the same time, a new generation of intelligent decentralized autonomous systems has been introduced, combining big data, information security, machine learning, artificial intelligence, and blockchain technologies to continuously promote and improve the construction of the entire ecosystem. The Internet of Everything, Interdependence, and Common Development 3.0 ecosystem.

2.5.3 Distribution Plan

he global value chain GVC has a constant total of 240 million pieces, 51% for mine mining, 21% for pre-subscription, 10% for operation team construction, 9% for foundation retention, and 9% for community construction.



The global value chain GVC pre-subscription began in May 2018. All subscriptions were exchanged using Time Chain TCC as the only token, and 21% of the subscriptions, namely 50.4 million GVCs, were completed in three phases. The subscription time was early in May. - In July, it is expected to exchange 3,840,000 TCCs, as follows:

The above time and exchange ratio will be adjusted according to the specific market conditions. Please refer to the official announcement.

2.6 Development Team

JOHN

John is a startup and technology attorney based in San Francisco, where he founded the law firm Experience Legal. John began his legal career as a capital markets associate in the New York office of Morrison & Foerster LLP and later started exclusively representing startups and technology companies in the Silicon Valley office of Orrick, Herrington & Sutcliffe LLP. Given this experience at the intersection of technology, innovation and capital markets, John has been at the forefront of alternative capital formation and securities regulation, most recently for blockchain startups raising capital through token sales.

DAVID

David is currently a research scientist at the MIT Media Lab' s Human Dynamics Group. He is also Co-Founder and Executive Director of ID3. Previously, David was Founder and Co-director of The Law Lab at Harvard University. He is also a member of the eG8 Forum and the Global Leadership Telco Council and the Risk Analysis Network for the World Economic Forum.

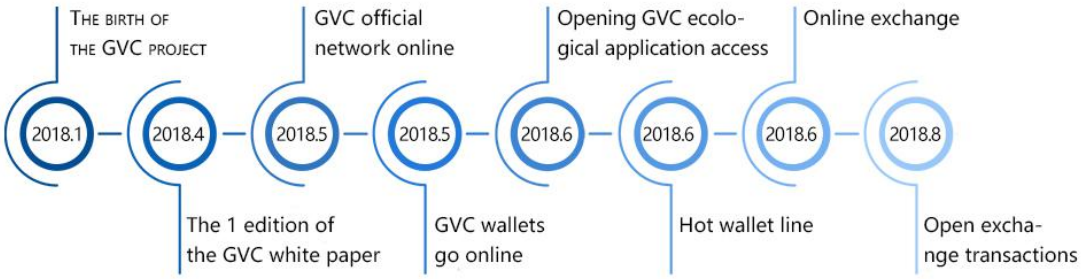
FRÉDÉRIC

SENIOR SOFTWARE ENGINEER
MIT D-LAB | 15+ YEARS OF SOFTWARE DEVELOPMENT

GRAU

SENIOR SOFTWARE ENGINEER
QUANT TRADING | 10+ YEARS OF SOFTWARE DEVELOPMENT

2.7 Development Plan



Part III Project Funding

The foundation of the GVC project was established in 2018 as the GVC Global Foundation. The Foundation is committed to the development of the GVC project and the value of the IoT ecosystem. The initial amount of 10% of GVC will be used for some industry applications and start-up projects, such as financial services, supply chain, Internet of Things, blockchain, etc. , Including project strategic planning, project support, project promotion, token exchange, community construction and the construction of the ecosystem.

The daily management decisions of the Foundation are implemented by the Council, which consists of the GVC Strategic Planning Committee, the Technology Development Committee, the Project Operation Supervision Committee, the Community Construction Management Committee, and the Finance Personnel Management Committee. Board members are recommended by the subordinate agencies.

The foundation will also set up special funds for rewarding excellent team members and support programs for outstanding projects, so as to supervise and support the sound operation of the entire project.

Part IV Risk Warning

For buyers participating in GVC, please carefully read the relevant descriptions of the GVC White Paper and the official website, fully understand the potential risks involved in participating in GVC, and fully combine their risk tolerance and actual conditions, make rational judgments, and make careful decisions.

Buyers should understand that GVC projects will not provide refunds under any circumstances. The GVC project team will, in accordance with the contents of the disclosed white paper, rationally use the digital assets it has raised, standardize the management projects, and do its utmost to ensure that the project is moving in the right direction. However, buyers still have the risk of loss. This includes:

(1) Policy Risk

At present, although most governments have a clear attitude toward blockchain-related industries and actively encourage them, the inherent loss of central blockchain attributes of public blockchains still faces many uncertainties at the level of government policies under the current centralized government laws and regulations. Sex.

(2) Market risk

The ultimate goal of GVC is to realize the free flow of decentralized values in the blockchain system. The future of the project will face various market challenges.

(3) Funding Risk

The capital risk refers to the major loss of project funds, such as the theft of funds, the inability to complete the development progress due to personnel and funding problems within a predetermined time, and so on.

(4) Risk of hacking or theft

Hackers or other organizations or countries have the possibility to try to interrupt the functions of the era chain in any way, including service attacks, Sybil attacks, raids, malware attacks or consistency attacks.

(5) Vulnerability risk or password science advances by leaps and bounds

The rapid development of cryptography or the development of science and technology such as the development of quantum computers, or the risk of hacking to encrypted tokens and GVC.

Part V Disclaimer

This document is for the sole purpose of conveying information and does not constitute an offer to buy or sell GVC. The above information or analysis does not constitute an investment decision. This document does not constitute any investment advice, investment intentions or teaching investment.

This document does not constitute or understand any act of offering or any

invitation to buy or sell securities of any kind, nor is it a contract or commitment of any kind. Relevant intention customers clearly understand the risks of GVC. Once investors participate in the investment, they understand and accept the risk of the project, and are willing to personally bear all the corresponding results or consequences.

The GVC team does not assume any direct or indirect loss of assets caused by participating in the GVC project.

GVC team

April 2018