GMC Technical Whitepaper

Global Industry Common Collaboration Platform

Foreword

Blockchain will be another new information revolution after the Internet. To a certain extent, it will change the existing production relations and business logic like the Internet, and then promote the high-quality development of human society.

Why is blockchain an information revolution? What exactly can this technology do?

Blockchain, as an important role in building the future value Internet, deeply integrates cutting-edge technologies such as distributed storage, point-to-point communication, distributed architecture, consensus mechanism, and cryptography. Countries around the world are speeding up the deployment of blockchain technology to promote technological innovation and industrial change. After the evolution of the blockchain project represented by Bitcoin to more than ten years now, the current underlying blockchain technology has become more mature and mature, and various blockchain solutions have covered various industrial applications and innovative applications worldwide.

In a wide range of user scenarios, technical challenges from performance, security, cost, expansion, etc. have become increasingly severe. At present, the interoperability between different blockchain applications is insufficient, and credible data circulation and value exchange cannot be effectively performed. Various blockchain applications are like isolated islands, and this phenomenon has greatly hindered the development of blockchain application ecology and integration. In the future, the blockchain wants to realize the true value of the Internet, assume the mission of transmitting trust, and open the era of all chains interconnection. It needs a universal, efficient, and secure blockchain collaboration mechanism to achieve cross-scenario, regional, and industry And so on.

The Global Industry Common Collaboration Platform is a platform developed based on blockchain technology and fully open source, referred to as GMC. It will work to promote trust transfer and business cooperation across industries, institutions and geographies. GMC is not limited to meeting the need for trusted data exchange after the parallel expansion of homogeneous blockchains, but also further explores effective solutions to solve the problem of inability to interconnect and interoperate due to the multidimensional heterogeneity of the underlying architecture, data structure, interface protocols, and security mechanisms among heterogeneous blockchains.

Blockchain technology is helping to create a better future world, and innovation in each application and technological progress are driving this process. Although there is still a long way to go before all issues are resolved, the inclusiveness and tolerance of blockchain technology has made people see the future. GMC will work closely with

users in various industries around the world to make the most of the cross-epoch significance in realizing the core commitment of the blockchain to give people a better future.

GMC Global Blockchain Team

Content

A. New ideas from digital currency to blockchain technology

We have entered the third decade of the 21st century. No one can really anticipate what events in the third decade will affect and change the world's economic, political, social and ecological systems. However, one can be sure that human economic activity will continue and that currency will not disappear in the next ten years. It's just that the currency will change significantly in the next decade. It has been learned that money is the most powerful force in the world, surpassing any economic, military and political force. Now it is time to look at the currency in a historical perspective, look for the all-round difference between digital currency and traditional currency, and show the historical moment of human currency evolution. However, existing monetary theory is not enough to accomplish such a historical mission. Therefore, new ideological resources need to be introduced to inspire, interpret, and recognize the evolution, status, and trends of money.

A.1 Biology of Genetics and Variation

Thousands of years of human currency history prove that currency has an unimaginable tenacious vitality. From its origin, its development and evolution have never stopped. If we recognize the history of money as a continuous process and the inherent "genetic" mechanism of money, we have to ask the question: Does money have an inherent "gene"? If so, what is this "gene"?

People agree that money originated from the "slate economy" of the two river basins in the Bronze Age 3000 years ago. Palaces and temples were the main economic entities, and money was created as a means of debt repayment. Nowadays, the debt currency supports the Fiat Money system commonly used by major countries in the world. Money is just an IOU. Can we say that "IOU" is the gene of money? There is also an empirical proof of the origin of the currency: the "stone coin" used by the residents of the "Yapu Island" in the Pacific, which the locals called "Fei". The island has a long history, and prior to the modern invasion, the island's inhabitants represented wealth by the number and size of the stones they owned.

There is such a story, a family once owned a huge "stone coin", which was sinking into the sea on the way back to Yapu Island. Despite this, other residents acknowledged that the family actually owned the wealth represented by the stone coin. It is no exaggeration to say that this case reveals the "gene" nature of money, that is, the "value" that people often say. Such "value" can be reflected in the transaction process, and it can also exist in the mind.

Genes are the basic unit of inheritance of living beings on Earth. In the biological world, "heredity" is not absolute, and genes are very likely to undergo structural changes, leading to genetic mutations. Because of heredity, the relative stability of species can be maintained; because of mutation, it may lead to the evolution of species

and the creation of new species. This theory can be verified in the history of money. From the perspective of the origin of money, the "IOU" and "value" of money are inseparable, which is likely to be the gene of the currency, and then form a unique DNA, which makes the currency have a strong "replication" characteristic and supports the stability of currency. one side. In this book, Long Baitao focuses on analyzing the operating mechanism of commercial banks and modern central banks based on the "loan to create money" theory, and uses various financial phenomena in the field of digital currencies to indeed touch the underlying mechanism of currency evolution.

A.2 Enlightenment of quantum features

In the "quantum mechanics" literature, no one seems to object to the "superposition", "measurement" and "entanglement" of the three characteristics, and these three characteristics completely violate people's common sense of understanding the macro world. In other words, no similar phenomenon can be found in classical mechanics. The so-called "quantum superposition" means that a quantum system can be in different quantum states. The so-called "quantum measurement" means that the quantum will change its existence state because it is measured. In other words, in the quantum world, any external measurement and observation will cause quantum uncertainty. The so-called "quantum entanglement" means that in a quantum system, although there is no force or connection between two particles, any changes to the quantum state of one particle still occur, and the other will immediately feel And make changes accordingly. That is, when the characteristics of each particle have been integrated into a whole, it is no longer possible to describe the characteristics of each particle individually.

In all human economic activities, currency is closest to the "superposition", "measurement", and "entanglement" characteristics: currency has always existed in different forms at the same time. Historically, such as gold, silver, and copper can exist as money at the same time; now, digital currencies and non-digital currencies coexist, thereby forming a "money superposition" phenomenon that exceeds "quantum superposition". Currency can also change due to different "measurement" criteria. For example, gold and silver have changed because of the "gold standard" or "silver standard" measurement scale. For another example, interest is also the "measurement" standard for money. Changes in interest absolutely affect the value structure of the currency itself. Currency has a strong nature of entanglement. The exchange rate is the most typical phenomenon of currency entanglement. The fluctuation of the value of any one currency affects the value of at least one other currency. In today's world, it is almost impossible to cut the world's major currencies from the world monetary system.

A.3 Catastrophe theory

There are two entry points for understanding the "mutation theory". First, the structural stability and morphogenesis published by French mathematician René Thom (1923-2002) in 1972 as the framework of a "catastrophic theory", which holds that There is a distinction between a stable state and an unsteady state in a state of movement. The "abrupt change" refers to the process of transitioning from one stable configuration to another. Or as defined, the transformation of a

non-linear system from one stable state (equilibrium state) to another stable state occurs in the form of a "mutation". Once "mutation" occurs, it is irreversible and a new stability can replace the original stability. Second, based on the biological "gene mutation" theory, "mutation" belongs to an extreme state of "mutation." "Gene mutation" has the characteristics of universality, randomness, low frequency, harmfulness and non-direction. The book <What is life? >puts forward: the stability of life and heredity and mutation under radiation (jump-like mutations) (jump-like mutations), indicating that life is subject to quantum laws. The common point of the above two types of "mutation theory" is that the evolution of nature and human social systems has always been non-linear, and both can cause mutations due to internal and external reasons. If you use the "catastrophic theory" to interpret the history of currency evolution, you will find too many "catastrophic" phenomena. The proposals and resolutions of the Blington Forest Conference belong to the "abrupt changes" in the global monetary system. In the past ten years, the formation of a digital currency group led by Bitcoin has been a larger "mutation". This "abrupt change" not only reflects the increasing influence of technology from the outside, but also shows that the currency itself has a non-linear evolution mechanism. It remains to be seen how central bank digital currencies will lead to the "alienation" of traditional currencies and even stimulate the "mutation" of the current digital currency system.

A.4 Chaos Theory

Edward Norton Lorenz (1917-2008) was recognized as the founder of this theory in 1963. However, although chaos theory has spread for many years, there is still no definition of "chaos theory" generally accepted by scientists, and scientists in different fields often have different understandings of it. However, there is almost no controversy about this cognition: "Chaos theory" is a theoretical system in the field of mathematics and physics that studies linear systems. Its most significant contribution is the use of simple models to derive explicit, periodic results.Uncertain, non-repeatable, random irregular movements, unpredictable phenomena, or "chaotic effects" existing in nature and society have been included in the research scope of "chaos theory". In addition, the chaotic changes in the initial conditions proposed by the "Chaos Theory" have been continuously exaggerated, and the theory that their future state will make a huge difference, especially the "butterfly effect" described by Lorentz has been widely recognized. After entering the information society and the digital economy, currency has the characteristics of increasingly strong uncertainty, non-repeatable, random and irregular movements, and often conforms to the "chaos theory" framework. Therefore, using the "chaos theory" to interpret currency phenomena will be greatly stimulated. The most typical case: The post-Blington Forest meeting's world currency system has become increasingly unpredictable and has such "disorderly" characteristics. Since the 1990s, because modern governments and central banks have become more and more subject to the influence of transnational capital, it has led to the frequency and destruction of global and regional financial crises, which has exacerbated the "disorder" of the global monetary economy. In addition, too many things demonstrate that any minor error in the central bank's monetary policy, because of the so-called "butterfly effect", may eventually threaten the security foundation of the entire international currency. From the cause to the result of the 2008 world

financial crisis, it is a process of constantly magnifying errors in monetary policy and the financial system. Later, it was difficult to explain the logic of the crisis.

A.5 Psychology

The combination of psychology and money should be said to have started with the American economist Irving Fisher (1867-1947). Fisher's "currency illusion" theory in 1928 revealed that people are accustomed to respond to the nominal value of money and ignore the specific psychological illusion of their actual purchasing power changes. Fisher wants people to get rid of the "money illusion" and focus on the purchasing power and potential value of money. Now, not only do people continue to be trapped in "currency illusions", but the government is even more conscious of using the people's "currency illusions" to implement inflation policies. In recent years, because of the combination of psychology and monetary phenomena, the Psychology of Money has emerged. As far as most related books and articles are concerned, "Money Psychology" is concentrated in the so-called wealth management category. Because of the inherent connection between psychology and behavioral science, there should actually be a "monetary behavior". In human history, never before has the "general public" cared about money and finance so much, and has never had such close effects as the "Cantilon" effect on people's lives. From the birth to growth of digital currency, the interactive relationship with people's belief and identification of the wealth form in the digital economy era emphasizes the relationship that smart contracts of the blockchain help to take into account fairness and efficiency, describes the sharing of coin tax, and achieves inclusive benefits finance, and the prospect of digital democratization. It is really important to adjust people's "psychological expectations" about monetary wealth. History has proven time and again that changes in the psychology and behavior of people's economy and wealth will have an underestimated impact on social transformation and constitute a deep driving force for the great social transformation.

In the face of the rapidly developing digital economy and digital currency, in the face of rapidly developing science and technology, and in the face of rapid social transformation, the limitations of the traditional currency theory from neo-classical to Keynes are obvious, and it is in awkward position. Georg Simmel (1858-1918), a currency philosopher, had hoped to "understand" modern life with the help of "money", so "our task is not to complain or tolerate, but to understand." After that, Simmel's mission still exists. Now we need to understand the digital age through the digital currency, understand the digital economy through the digital age, and then understand the digitized era and culture through the combination of the digital economy and digital currency. To recognize digital currency, we need to use and introduce new ideological resources, and gradually form a new currency theory.

B. The design background and concept of GMC

Combined with the "new ideas from digital currency to blockchain technology" above, it is enough to prove that currency is a cross-industry, regional, and ethnic medium that has never been disputed since the history of human civilization. But now, digital currency-oriented blockchain technology has failed to break through this phenomenon. Therefore, digital currency is not the greatest implementation of blockchain technology in the future, but it is to find a blockchain technology solution similar to currency that can realize obstacles across industries and regions.

B.1 Design Background: Industry Status and Challenges

In recent years, the blockchain industry has experienced rapid development, and many low-level technology platforms have been born. Blockchain applications based on these platforms have emerged. With the development and expansion of the application ecology, more and more applications are based on existing users and value accumulation. In order to pursue greater network effects, there is a need to interact and establish relationships with other applications. Therefore, the entire blockchain ecosystem needs a more open, collaborative, and win-win interactive environment. Due to the multi-dimensional heterogeneity of the current blockchain platform technology implementation, there is an "island effect" in applications and data. Regardless of different applications built on different platforms or the same platform, it is difficult to easily achieve cross-platform Uni-com collaboration. The evolution of the blockchain ecosystem to the next stage requires innovative solutions that "beyond platforms and link applications."

To address this challenge, cross-chain technology, which aims to build a trusted interaction channel between chains, has gradually become the focus of attention in the industry. The industry generally agrees that efficient and versatile cross-chain technology is the key to achieving Wanchain interconnection. Cross-chain technology can connect the scattered blockchain ecological islands and become a bridge link for the overall outward expansion of the blockchain.

Currently, the industry has made preliminary explorations and accumulations in the cross-chain field. More cross-chain schemes have been discussed including notary mechanism, relay, side chain, hash lock, and distributed key control. Earlier BTC-Relay used side chain technology to achieve one-way cross-chain between blockchain digital assets. The cross-chain value transfer protocol ILP proposed by Ripple uses a hash lock solution to solve the problem of cross-ledger payment. Cosmos and Polkadot focus on how to establish a universal cross-chain development framework. They have proposed the development frameworks of Tendermint and Substrate, respectively. The cross-chain technology design is based on the idea of a relay chain.

The above-mentioned cross-chain solution is only applicable to cross-chain transfer scenarios for digital assets, but it is difficult to expand to cover wider application scenarios. As early as 2015, the GMC team has proposed the "industry general collaboration" blockchain concept, which further promotes the blockchain to all industries worldwide. The industry serves as the "chain" and can access the "chain" through an open network. The service provided by the industry is the

owner and operator of the "chain", which realizes the exchange of information and value through the "chain".

GMC is not a single blockchain ecosystem, but a new cross-domain integration form of the blockchain industry. To support such a converged form, it needs to be able to support multi-chain parallel, cross-chain communication, and the ability to process massive transactions from the Internet. In this big ecosystem realized by blockchain, it is necessary to deal with the characteristics of heterogeneity of the underlying platform and diversified application scenarios, etc., building a cross-industry universal blockchain ecosystem to realize trusted interaction will face greater challenges.

B.1.1 Different underlying architectures make interoperability difficult

There are a variety of blockchain platforms in the industry. These platforms differ greatly in their overall architecture design, including various aspects such as computing, storage, and networking. For example, Bitcoin, the pioneer of blockchain technology applications, has an underlying architecture. The design uses Unspent Transaction Outputs, referred to as UTXO, which is the last-spent transaction output. In the bitcoin world, there is no account book that records all account balances. So how do you determine how much balance an address has now? Simply put, you need to review all previous transactions, find all the bitcoins sent to you, and add them all up before you know. The account model used by Ethereum, known as the Blockchain 2.0 era, is easier to understand, as if we each have a bank account. In the world of Ethereum, each address is like an account. After each transaction, the balance of the account will be recorded in the blockchain. Therefore, it is sufficient to check whether the account has sufficient balance when authenticating the transaction. Hyperledger Fabric adopts the Endorser-Orderer-Comitter three-layer architecture. The transaction is pre-executed and endorsed by the Endorser node, and the status read-write set RW-Set is returned to the client. The client then packages the transaction and sends it to the Orderer. The node performs disk storage. It is not difficult to see that there is a huge difference in the architecture of the three platforms. Not only are the transaction processing timings different, but the calculation and storage structures are different. There are huge challenges to make transactions directly interoperable on the three platforms.

B.1.2 Different data structures make mutual recognition difficult

The data structure design of different blockchain platforms is often different. For example: Bitcoin uses a single binary tree composed of cryptographic hashes, called a Merkle tree. Ethereum uses an optimized Merkel Patricia tree, which is characterized by a data structure containing four trees in the block header: State Trie, Storage Trie, Transaction-Trie, Receivets-Trie and Hyperledger Fabric. Taking its latest stable release as an example, a DataHash field is used to mark the data changes of the block. The block header design does not have related fields of the Merkle Tree, and it is not easy to implement a similar transaction existence proof mechanism. The existence verification based on Merkle Tree is a commonly used cross-chain authentication method, but because different blockchain platforms have different data structures and expected application scenarios, not all platforms support it, so there are still certain challenges in achieving mutual recognition of data.

B.1.3 Different interface protocols make interconnection difficult

Common network transmission encoding protocols include Protobuf, JSON, and binary system. These encoding protocols each have their advantages and applicable scenarios. For example: Bitcoin uses JSON-RPC for data transmission. The Protobuf protocol has the advantages of supporting multiple languages, compact format, and easy to expand. It was selected by Hyperledger Fabric as the encoding protocol for P2P network transmission message packets. In addition, because the architecture and data structure are different, the access interfaces exposed by different platforms are also very different in terms of functions and format fields. In summary, due to the incompatibility between the interface and the protocol, it is difficult for these platforms to communicate with each other.

B.1.4 Different security mechanisms make mutual trust difficult

Blockchain security covers a wide range of aspects, including the security of consensus accounting models, data transmission security, data storage security, access mechanism security, and interface access authority security control. Because the security boundary of the blockchain design is often based on the platform's scope, to ensure that a blockchain instance built with this platform is secure inside. When it comes to chain-to-chain, platform-to-platform connection, various security mechanisms are uneven, and sensitive data cross security boundaries, such as different consensus lists, strict admission mechanisms, high and low levels of authority, the differences in permissions, and other factors lead to the failure of the mutual trust conditions between the platforms.

B.1.5 Different business models make mutual visits difficult

Blockchain technology has emerged in many application areas. Take the application scenario of Ethereum in smart contracts as an example, which can cover government, finance, traceability, culture, games and many other industries. The contract logic for different business scenarios varies widely, and each scenario is an internal closed-loop system. To open up mutual visits between scenarios, for example, to achieve the cross-chain interoperability of record-related information in the financial scenario blockchain and government affairs blockchain, it will face more complex business logic than traditional data asset cross-chain. Omissions in any part of the process may cause exceptions to make cross-chain failures. How to ensure the integrity and consistency between transactions and transactions in the overall connection process will be a huge challenge.

In addition to the aforementioned challenges due to differences in the architecture of different platforms, there are also significant cross-chain challenges between multiple blockchains based on the same blockchain platform. Limited by the architectural characteristics of the blockchain itself, the single-chain architecture cannot meet the three requirements of high security, high performance, and high expansion at the same time, and it cannot cope with service scenarios that need to carry large amounts of data. Although traditional Internet services can be used for reference, blockchain applications are a weakly trusted business model with multiple parties involved, and there are both collaborations and games between multiple parties. Even for blockchain applications built on the same platform, it is also necessary to build a multi-party

trusted channel to interconnect the trusted data of channels, groups and multiple chains after equal expansion.

Therefore, both homogeneous / heterogeneous blockchain platforms need to rely on cross-chain solutions to connect islands of trust, realize the transmission of trust in a wider range, and promote the deep integration and development of blockchain application ecology.

B.2 Design Concept: 5S Principle

Facing the many challenges of interconnection and interoperability in the blockchain application ecosystem, the GMC team began to think deeply about the underlying architecture design, and explored the "minimum" abstraction design required for credible integration and connectivity in many mainstream platforms, fully considering the security, expansion, and usability issues of cross-industry collaboration and interaction, and propose targeted solutions that follow the 5S principle.

B.2.1 Synergetic: Cross-industry collaboration

The goal of building a universal industry collaboration is to open up the high walls between various industries, connect many islands of trust, and allow trust to be passed on to a wider range. In order to enable these businesses based on many different industries to work together seamlessly, first of all, a common data structure and interaction protocol need to be designed to minimize the cost of data format conversion and adaptation between different industries.

GMC follows the design concept of meeting efficient cross-industry business collaboration. According to the principle of "one-time adaptation, available everywhere", the "core interface subset" necessary for cross-industry interaction is refined, and data structures and network protocols can be designed to solve the problem of interface differences between platforms in different industries due to different design goals.

B.2.2 Secure：Cross-industry interoperability

One of the important characteristics of the blockchain is to achieve trusted access to data through decentralization, consensus mechanisms, and cryptography. But this security mechanism often can only form a closed loop inside a blockchain platform. When conducting interactive access between two or more blockchain platforms, it is necessary to further break through the security boundaries of the original platform and establish a stronger security guarantee mechanism.

GMC follows the design concept of ensuring cross-platform operation security and credibility, introducing the CA identity authentication mechanism, encrypting and strengthening communication links, strictly restricting access permissions, designing a multidimensional Merkle proof mechanism, and a variety of atomic transaction mechanisms to ensure the trust of full-process data across platforms and chains.

B.2.3 Scalable: Cross-chain network layered and scalable

Cross-chain can not only support interconnection between heterogeneous blockchains, but also help expand the homogeneous blockchain platform. Common multi-channel, multi-group, and multi-chain expansion schemes need to rely on cross-chain components to open channels, groups, and chain-to-chain interactions. With the evolution of cross-chain business collaboration, more and more services have interconnected requirements, and one-to-one cross-chains will evolve into one-to-many, many-to-many, and even more complex topologies. This requires that the cross-chain components themselves have sufficient flexibility to be able to cope with a variety of complex network models and business requirements.

GMC follows the design concept of supporting hierarchical expansion of cross-chain networks, designing cross-link protocols and modules. This module supports distributed interconnection of multiple blockchains, bears various topologies such as tree and star, and supports multi-level deep cross-chain collaboration. At the same time, design a multi-party co-construction and co-governance governance architecture to achieve the sustainable expansion of cross-chain networks.

B.2.4 Swift: Efficient and convenient cross-link entry

Due to the diverse characteristics of the blockchain platform, developers need to learn a set of blockchain development operation and maintenance processes every time they access a new blockchain platform. Access across different blockchain platforms will lead to increased learning costs.

GMC follows the concept of providing developers with efficient and convenient access methods. It designs a full set of development components such as SDK, interactive console, and visual browser to simplify cross-chain interactive processes and design "what you see is what you get" operation and maintenance tools, which will supports one chain to initiate cross-chain operations.

B.2.5 Store: Cross-industry data distributed storage

Except for Bitcoin and Ethereum, the blockchain industry currently does not have a true public chain, which belongs to the category of alliance chain. As a true public chain, Bitcoin and Ethereum have the disadvantage that the threshold for building a node is very high, and it can only be completed by a professional and experienced developer of the relevant program, and the synchronization process is very slow. At present, other alliance chain platforms on the market with public chains only have the function of super nodes. If there is a problem with the super node, the data will be irreparably damaged, and if this type of alliance chain wants to build a node, it also has the disadvantage of high threshold.

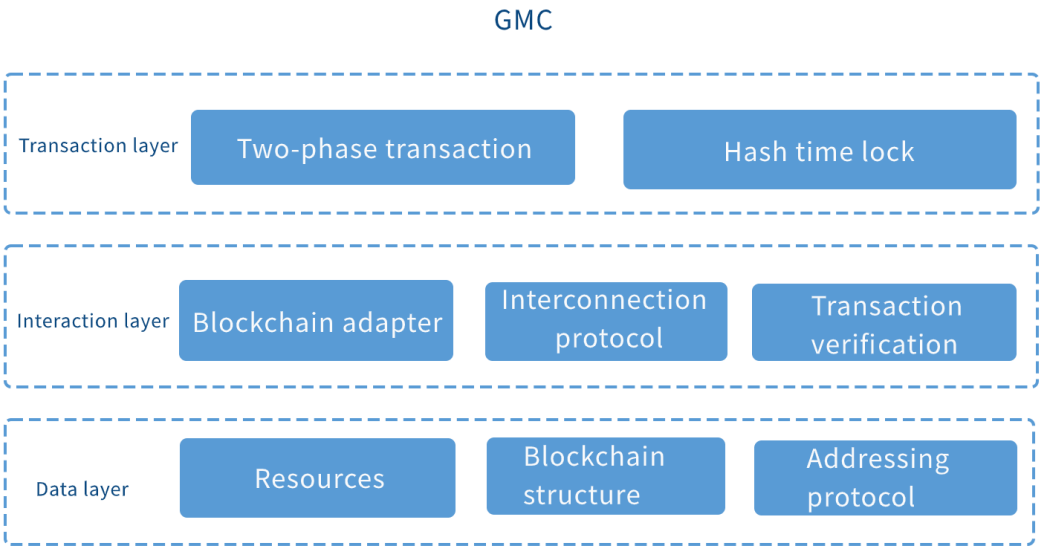
GMC follows the concept of distributed storage in the blockchain. In the underlying design, the concept of super nodes is introduced in order to support high performance, and the design of devices as nodes is also referenced. Users can build nodes with one click in the visual operation component without the need of professional developers .

C. GMC overall architecture design

With the goal of integrating and connecting major mainstream blockchain platforms in various industries, based on a comprehensive analysis of the current global industry status, application scenarios and development of blockchain technology, GMC has standardized and abstracted the mainstream blockchain platform system, and restructured the overall architecture.

C.1 Blockchain system abstraction

In order to enable interaction between heterogeneous platforms, a unified "language" is first designed for these heterogeneous blockchains, that is, a unified architecture. Only by finding a "language" that both parties can understand between heterogeneous blockchains can interconnection be realized. Based on the key requirements needed for cross-chain, GMC abstracts the core public platform's core and necessary public subset of the mainstream blockchain products in the core data structure, blockchain interaction mode, and transaction management, and abstracts the blockchain platform at multiple levels.



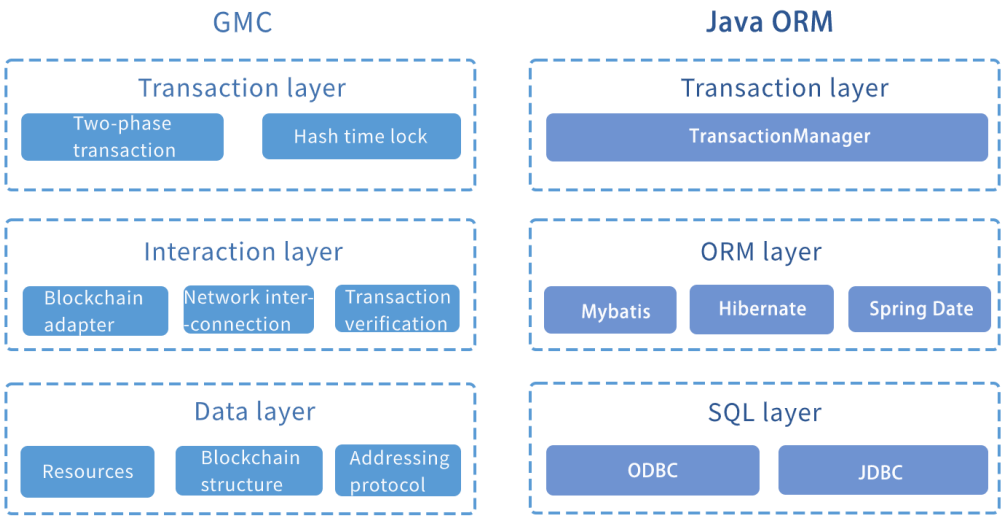
Data layer: The core of cross-chain interaction is the flow of data between chains. The abstraction of the data layer is particularly important. The data dimensions involved in cross-chain include blocks, transactions, contracts, and messages. GMC meets the basic requirements of cross-chain as a prerequisite, refining common block data structures, abstracting transactions, contracts, and messages into resource types, and designing general addressing protocols for resources.

Interaction layer: Different business scenarios have different cross-chain interaction models. Based on the abstract data layer, GMC builds a universal blockchain adaptation and routing relay network, and combines the standard Merkle proof mechanism to achieve the abstract design of the cross-chain interaction layer.

Transaction layer: An abstraction layer based on data structure and interaction to achieve the effect of cross-chain transactions. Two types of mechanisms are currently supported: two-phase transactions and hash-time-locked transactions. In the future, more transaction mechanisms will be designed according to the needs of the scenario.

Any layer in the GMC abstract architecture is universally replaceable, and the logic of the upper layer can be universally used regardless of how the underlying technology is replaced. GMC's multi-level abstraction of the blockchain can be compared to the Java ORM (Object Relational Mapping) multi-level abstraction of the database. ORM technology, as a common "language" for Java to access the database, can completely hide the database layer and present only the Java objects developed. Developers only need to call the method of the Java object according to the needs of business logic to implement the operation of the background database, without having to pay attention to what database is used in the background. Correspondingly, the GMC data structure abstraction can correspond to the SQL and database-driven abstractions in Java such as ODBC and JDBC.

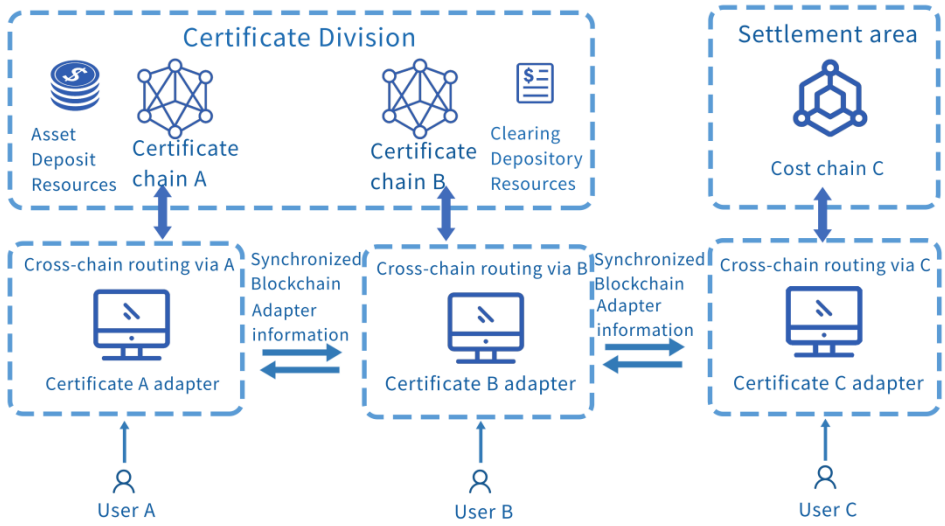
GMC interaction abstraction is similar to Java's ORM abstraction of database access models such as MyBatis and Hibernate, while GMC transaction management is similar to Java's transaction management, but supports more transaction modes.



C.2 Cross-chain system architecture

GMC's cross-chain system architecture design fully considers multi-blockchain interconnection across industries, institutions and regions. Whether it is a newly deployed blockchain platform or an existing blockchain platform, it can be based on the abstraction of the blockchain system in the previous section, and seamlessly connect GMC platform without changing the underlying layer of the original blockchain platform.

The GMC system architecture includes the following components:



Cross-chain zone (Zone):

Refers to a collection of blockchains running the same type of business. GMC can name and address this blockchain collection itself and internal blockchain resources. For example, in the figure, the namespace of the depository business is "the depository partition", and the namespace of the training business is "the settlement partition". There are two certificate chains in the certificate deposit zone, namely certificate chain A and certificate chain B. An asset certificate resource is deployed on the certificate chain A chain, and the costs and related assets may need to be certificated. Therefore, according to business needs, cross-chain operations will result in partitions and between partitions, and between chains and chains within partitions.

Cross-link by (Router):

Refers to the service process used to bridge business systems with the blockchain. Multiple cross-links can be connected to each other and forward requests to each other. The user accesses the resources in the cross-chain partition by initiating a request to the cross-link.

Cross-chain adapter (Stub):

Refers to the implementation of an interface connected to a blockchain, which can be configured by cross-link loading and cross-link. Multiple blockchain adapters can be configured to achieve the effect of connecting multiple blockchains. Cross-link routing will automatically synchronize the configuration information of the blockchain adapter to help users address resources located on other blockchains.

Cross-chain resources (Resource):

Refers to data objects accessible to users such as smart contracts and digital assets on the blockchain. Similar to the configuration information of the blockchain adapter, the

meta-information of cross-chain resources is also synchronized across the links. Users address and call resources in cross-chain partitions through a unified interface.

In order to meet the future diversified business interconnection requirements, GMC has set the following key design goals for the network interaction and deployment architecture based on the typical business characteristics of massive data cross-chain.

Cross-regional interconnection:

As a multi-participating blockchain application, it usually involves multiple service agencies, and the business is deployed in multiple cross-region data centers. GMC designs a secure, reliable, and efficient network architecture for cross-regional scenarios. The network mechanism based on TCP long connection, heartbeat, automatic reconnection, and encrypted communication technologies ensures the stability, timeliness, and security of wide-area cross-regional interconnection.

Flexible deployment architecture:

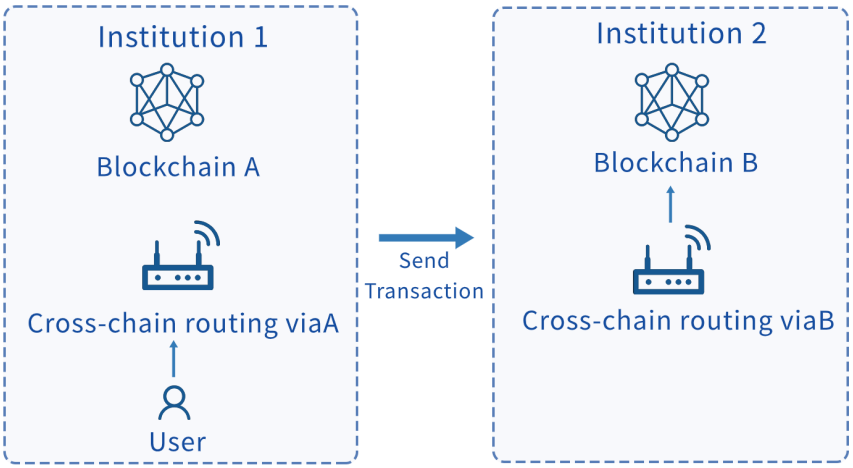
Because cross-chain requirements usually originate from mature blockchain application projects, cross-chain deployment architectures need to have the ability to be compatible with existing blockchain instances. GMC adopts a "non-intrusive" design, and cross-links are deployed separately from blockchain nodes in an independent process, and there is no need to change the existing blockchain network architecture to achieve flexible architecture deployment. Cross-link routers use the network to transmit cross-chain messages and blockchain messages. Combined with the automatic path finding function of the network, as long as the cross-link routers have direct or indirect reachable network links, cross-chain interaction can be completed.

Freely customizable:

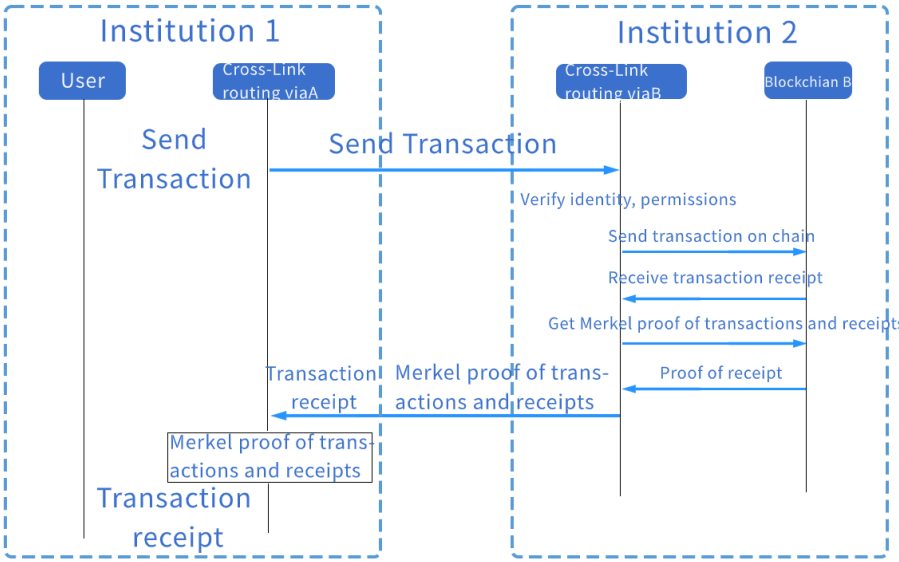
Cross-chain requirements in real-life business scenarios vary widely, and there are a variety of connected blockchain platforms, so customized and tailored cross-chain capabilities are essential. GMC's blockchain adapters and cross-chain resources support free customization. Depending on the type of blockchain, system resources and network conditions, different blockchain adapters and cross-chain resources are selected.

C.3 Trusted interaction process

The basic security assumption of the design of the blockchain platform is that "every participant may do evil". Under this assumption, a distributed and trusted environment is constructed through mechanisms such as cryptography and consensus algorithms. However, this trusted environment often only takes effect inside the blockchain platform and cannot be trusted simply by another blockchain platform. Additional trusted proof information needs to be introduced to achieve trusted interaction across blockchain platforms. In addition to transmitting blockchain transaction information when processing cross-chain interactions, GMC will additionally transmit relevant proof data of blockchain transactions, and use this information to prove the existence of transactions and receipts (transaction execution results) to prove the authenticity and reliability of the information on the chain.



The cross-chain interaction shown in the figure above is taken as an example. Institution 1 and Institution 2 have deployed Blockchain A and Blockchain B, respectively. Now the users of Mechanism 1 want to access the blockchain B of Institution 2 and require that the results of the visit be authentic and credible. The sequence of cross-chain interactions is shown in Figure below.



Compared with the traditional blockchain transaction processing process, GMC cross-link is certified by Merkel in addition to transmitting transaction and receipt information, as well as transmitting transactions and receipts. The sender of the transaction uses these certificates to perform credible verification of cross-chain data access, so that the sender of the transaction can confirm that the transaction actually occurred on the target blockchain and obtain results, and ensure that the transaction and receipt are authentic and credible.

GMC follows the principle that cross-chain interaction data can be self-certified, and requires interactive response messages to carry both data and certification. This rule is generally applicable

to various cross-chain scenarios and can be used to ensure the authenticity of the entire transaction process.

D、GMC core technologies and advantages

In order to achieve efficient availability, security, trustworthiness, and convenient governance of cross-chain interactions, GMC is based on the abstraction of the blockchain system, the top-level design of the cross-chain system architecture, and the trusted interaction process, refining four technical points to achieve the core of cross-chain features:

Universal Block Link Interface (UBI):
GMC designs a set of universal blockchain data protocols, abstracting and abstracting the core data structures and resource definitions common to mainstream blockchains, enabling multiple blockchain platforms to interact with a unified data protocol, greatly reducing the blockchain difficulty of interaction between platforms.

Boundary Chain Interconnection Protocol (HIP):
GMC designs common network interaction protocols and unified interaction modes for mainstream blockchain platforms. Through simple adaptation, the connectivity of heterogeneous blockchain platforms can be achieved.

Trusted transaction mechanism (TTM):
GMC uses cryptography and distributed algorithms to ensure the authenticity and reliability of the interactive data between the blockchain platforms and to prevent tampering, and the atomic transactional nature of business logic, enabling any two transactions associated with the blockchain platform to be able to fully executed or fully rolled back.

Multilateral Inter-Domain Governance (MIG):
GMC designs a set of extensible and decentralized cross-chain governance architecture, allowing multiple blockchain businesses to jointly build a governance chain for cross-chain interaction governance according to their specific needs which carries authority control, transaction management, Governance functions such as access mechanisms and regulatory intervention.

Byzantine Fault Tolerance – Delegated Proof Of Stake (BFT-DPOS):

GMC follows the CAP principle in the design of the consensus mechanism and uses the BFT-DPOS consensus mechanism to ensure system availability and partition fault tolerance.

Combining comprehensive considerations in design concepts, user experience, and platform features, GMC has the following three main advantages:

Open source and open: GMC adheres to the principles of open source and openness, maintains the iterative upgrade of the platform with the community, and works together to build a stronger and better cross-chain platform.

Development friendly: GMC provides multi-language versions of SDKs for developers to use, and provides visual management tools to facilitate user development, debugging, and operation and maintenance.

Security and credibility: GMC guarantees the confidentiality of cross-chain data and the security of the system based on multiple mechanisms such as encryption, access, isolation, and traceability.

D.1 Universal Block Link Port

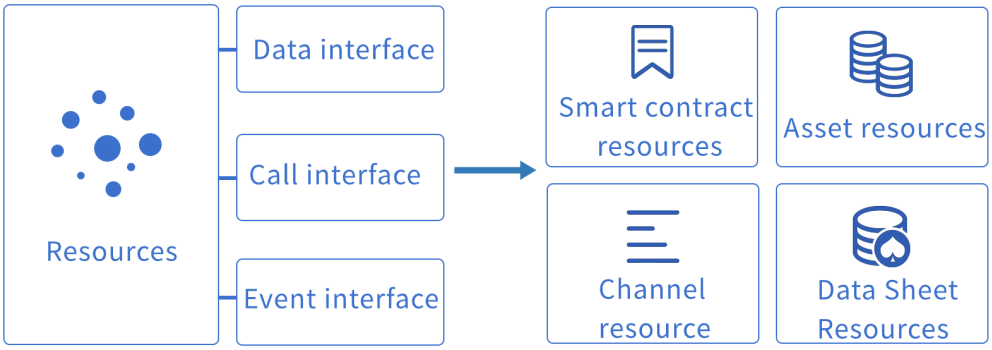
Each blockchain platform has its own SDK, smart contract framework, and interaction logic. Developers have to learn the API and calling logic of each blockchain platform for customized development. When cross-chain requirements exist between two heterogeneous platforms, bilateral businesses need to relearn the API and calling logic of the other platform. This is not only a huge waste of developer energy and cost, but also an important reason for the difficulty of landing across chains.

Although the blockchain platforms are different, they are inseparable, and the underlying principles of mainstream blockchains have something in common. After abstraction, the blockchain logic, block data structure, and transaction data structure of most blockchain platforms have high similarities.

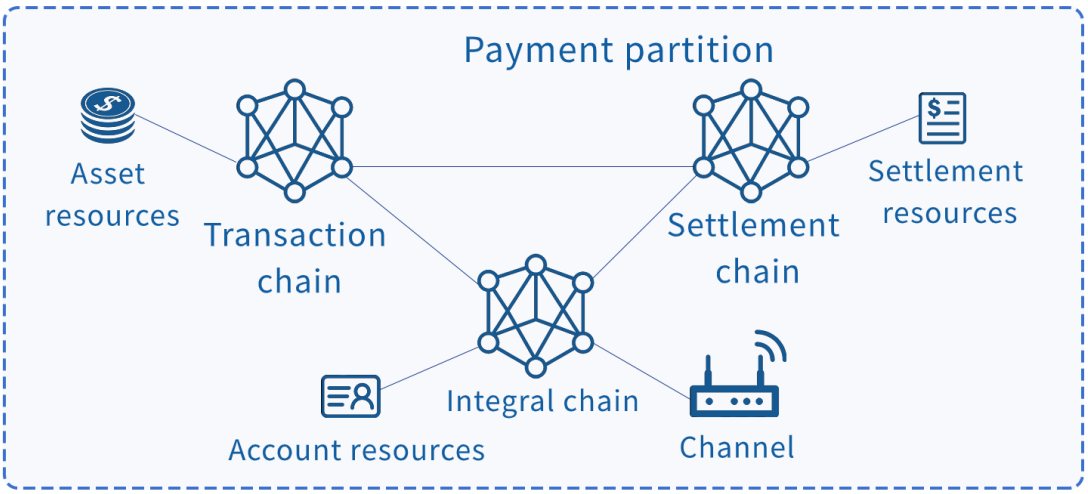
Based on the basic ideas of "seeking common ground while reserving differences" and "focusing on the greatest common divisor", the Universal Blockchain Interface (UBI) abstractly packages of data such as transactions, smart contracts, and assets, designs a unified resource paradigm, refines key data structures of mainstream blockchains, and designs abstract block data for universal cross-chain scenarios. The structure establishes a consistent data protocol foundation for the interaction of heterogeneous blockchains, and achieves the "one-time adaptation, available everywhere" effect.

D.1.1Uniform Resource Paradigm

The resources on various blockchain platforms are diverse, including smart contracts, assets, channels, and data. No matter how diverse the functions of these resources are, their core interfaces can be summarized into three types of fixed interfaces: data, calls, and events. In order to better open up the resource interaction of the blockchain platform, UBI proposes a unified resource interface paradigm so that users do not need to care about the specific smart contract language and the underlying architecture of the blockchain when calling blockchain smart contracts, assets, channels or data tables. They just need to pass in common parameters and handle uniformly defined return values.



Resources on a single blockchain can be located and accessed through contract addresses or names. Under the complex network model of cross-chain and multiple business interconnection, a higher-level resource positioning protocol is required. In order to allow users to locate and access blockchain resources under complex cross-chain partitions, they do not need to care about which region, institution or computer room the resource is located in, nor do they need to be concerned about the actual implementation of the blockchain. You only need to provide the resource address and related parameters to achieve resource positioning and access. UBI uses a unified resource addressing protocol, and implements an automatic routing and forwarding mechanism to intelligently locate the required resources for users.



GMC defines a cross-chain system as a combination of cross-chain partitions, business chains, and resources on the business chain. The payment partition in the figure above is taken as an example:

Cross-chain zone (Zone): It governs a number of business chains with a certain correlation. The correlation may include business models, regions, areas, and other payment partitions in the Q diagram.

Business chain (Chain): The business chain runs in a cross-chain partition and belongs to only one cross-chain partition. The transaction chain, point chain and settlement chain in the figure are all business chains in the payment partition.

Blockchain resource (Resource): refers to objects such as smart contracts and assets in the business chain. As shown in the figure, asset resources are resources of the transaction chain, settlement resources are resources of the settlement chain, and account resources are resources of the credit chain.

Cross-chain partitions, business chains, and blockchain resources are all uniquely identified. By combining three types of identifiers, you can uniquely locate the position of any resource in the cross-chain system. This addressing identifier is called the cross-chain path (iPath, Interchain Path), and the cross-chain path is defined as:

【Cross-chain zone (Zone)】-【Business chain (Chain)】-【Blockchain resource (Resource)】

Take the payment partition in the figure as an example:
Access the asset resources of the transaction chain, the cross-chain path is: payment partition. Transaction chain. Asset resources
Access the settlement resources of the settlement chain. The cross-chain path is: payment partition. Settlement chain. Settlement resources
Access the account resources of the credit chain, the cross-chain path is: payment partition. Credit chain. Account resources

GMC is designed to implement the HTTP Restful interface to access cross-chain paths, and supports access to resources in cross-chain systems in the form of HTTP URLs. The URL format is:

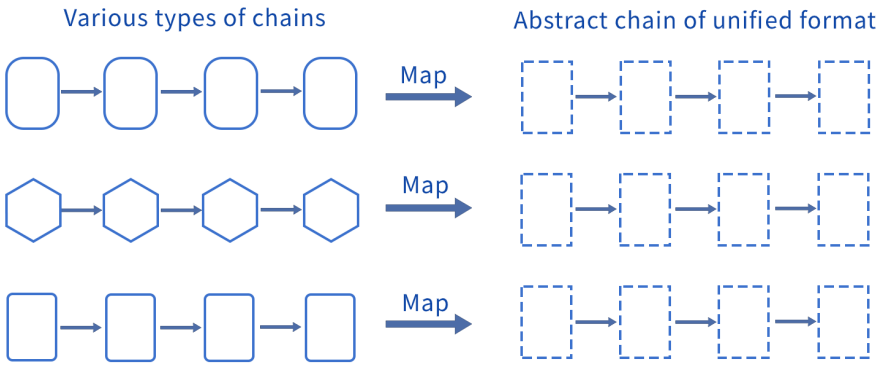
http://IP:Port/【Cross-chain zone (Zone)】/【Business chain (Chain)】/【Blockchain resource (Resource)】/【Resource Approach】

The call to a smart contract is called a call interface, which is divided into two types: call and sendTransaction. The call interface only uses the contract to read the interface to return data and does not change the state on the chain. SendTransaction sends transactions to the chain and changes the state of the blockchain. . There is also an event interface for customers to receive event events from smart contracts.

D.1.2 Abstract blockchain structure

In order to meet the need for mutual trust of block data between heterogeneous blockchains, UBI proposes the concept of abstract blocks. A chain composed of abstract blocks is called an "abstract chain". The abstract block contains data fields common to the mainstream blockchains in the industry, which are used to verify the correctness of the blockchain development, query the

current state of the blockchain, and verify blockchain data. Multiple blockchains can confirm the status of other blockchains and verify the correctness of the expected interaction data by synchronizing with each other and obtaining the abstract chain.



The data fields of the abstract block can be divided into two types. One type is the block information field, including block height, block hash value, and the previous block hash. These fields are used to verify the correctness of the blockchain. The other type is the information verification field, including transaction Merkel root, receipt Merkel root, and status Merkel root, which are used to verify the existence and correctness of the transaction, receipt, and status data related to the block. These prove whether a transaction belongs to the current block, whether a receipt is due to the current block, and so on.

D.2 Heterogeneous chain interconnection model

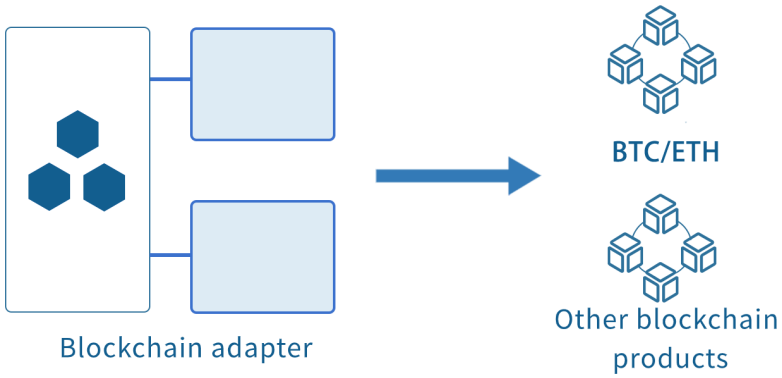
The core of blockchain interaction is interface calling. Although the internal architecture, network model, and consensus logic of each blockchain platform are very different, the external interfaces of these blockchain platforms have commonality. At least they all have interfaces such as data reading and writing, calling smart contracts, and sending transactions to smart contracts.

The Heterogeneous Chain Interconnection Model (HIP) analyzes the commonalities of the interaction methods of mainstream blockchain platforms, and refines a general block linking paradigm and cross-chain interaction model. With a small amount of adaptation and docking between blockchain platforms, cross-chain interactions between heterogeneous chains can be realized.

D.2.1 Universal access paradigm

HIP defines a general block chain entry paradigm, and only needs to implement two core interfaces to access a blockchain. These two interfaces are the interface to obtain "resources" and the interface to obtain "information". The resources are derived from the unified resource definition described in 3.1.1 "Uniform Resource Paradigm" section, and information is key information on the blockchain such as block and block height. Based on this general paradigm, different blockchain platforms can each provide a blockchain adapter (Stub). The blockchain adapter can be packaged based on the original blockchain platform SDK to achieve the core

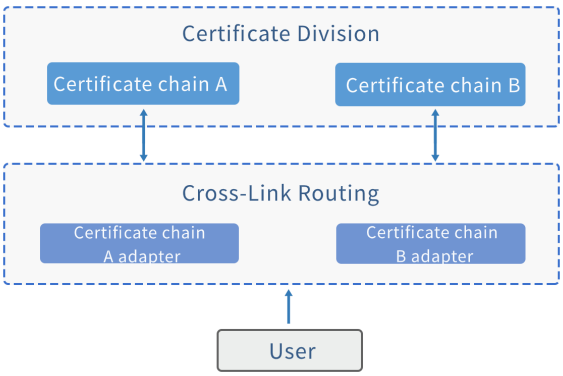
interface of HIP without the need to make infiltration modifications to the original blockchain. Any blockchain can access the GMC platform as long as it follows the blockchain link-in model and implements a blockchain adapter. The access method is loaded by a cross-link and blockchain adapter, so as to achieve access to the blockchain platform.



D.2.2 Cross-chain interaction model

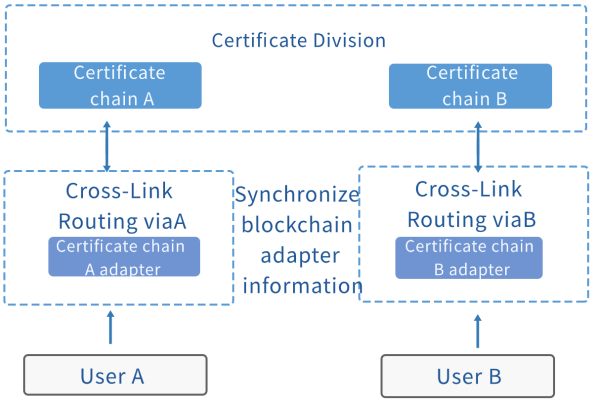
In order to adapt to the changing cross-chain business scenarios, HIP designs a set of cross-chain interaction models, which can support multiple scenarios such as single partition single routing, single partition multiple routing, and multiple partition multiple routing.

Single partition and single route: For the scenario where users of an organization need to visit multiple blockchains at the same time, you can set up a cross-link router in the organization and configure multiple blockchain adapters for it to connect to multiple blockchains. By configuring different iPath prefixes for multiple blockchain adapters, users can arbitrarily address and access resources in the network through cross-link routing. As shown in the figure, user A can access the resources on the two chains through the cross-link configuration of two different blockchain adapters.

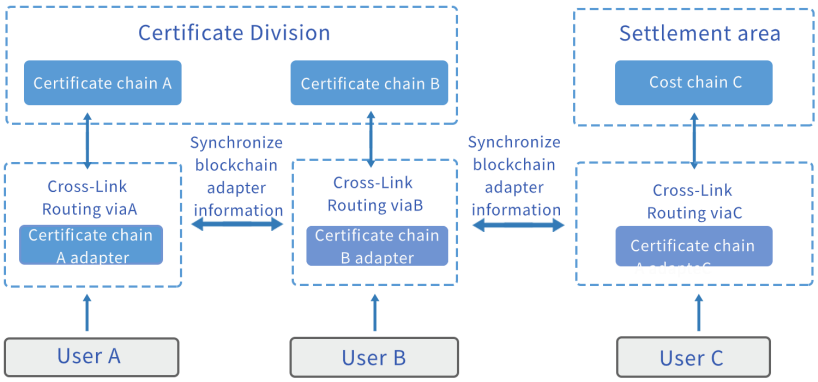


Single-zone multi-routing: For multiple users of multiple institutions who want to cross access each other's blockchain, they can all sign multiple cross-link routes and configure their own blockchain adapters. The cross-link routers are connected through a P2P network protocol, and the cross-link routers will automatically synchronize and exchange their respective blockchain adapter and resource information. Users of different institutions can call their own cross-link reasons, and

cross-link routes from their own institutions to forward cross-link reasons to other institutions, access corresponding resources, and return by routing. As shown in the figure, user A can access the resources on the two certificate management chains through a routing network consisting of cross-link viaA and cross-link viaB.



Multi-division and multi-routing: In more complex business scenarios, there is a need for multiple services to be integrated with each other, so there is a need for interconnection and access in multiple cross-chain partitions. In the face of this demand, HIP supports cross-links to dynamically increase connections with other cross-links. Through limit control, it ensures the security and control of cross-chain access, without any modification of the original business. As shown in the figure, the certificate partition and the settlement partition are connected by cross-links, so that users in the original two partitions can access the resources of the other partition.



As can be seen from the above three scenarios, cross-link is the core module of the entire interaction model and a bridge connecting multiple blockchains. Cross-links are deployed as independent processes. One cross-link can use multiple blockchain adapter modules to connect multiple blockchains, and multiple cross-links communicate with each other using a P2P network. Cross-linking uses the concept of hierarchical design from the inside and is divided into four levels from the bottom up:

Basic layer: The most basic part of the cross-link consists of the bottom layer, including network interconnection module, blockchain adapter module and abstract chain storage module. The network interconnection module is responsible for cross-link interconnection. The blockchain adapter module is responsible for connecting specific blockchain nodes. The abstract chain storage module saves the abstract block header information of multiple blockchains for verifying transactions and receipts.

Interaction layer: Handles the interaction logic of cross-links, including modules such as resource synchronization, resource addressing, and cross-chain certification. The resource synchronization module synchronizes multiple other cross-link resource configuration information. The resource addressing module helps users address resources by iPath in the cross-chain partition. The cross-chain certification module verifies the transaction and receipt data returned by other cross-links.

Transaction layer: Process and coordinate transaction logic across the blockchain, including two-phase transaction modules and hash time locking.

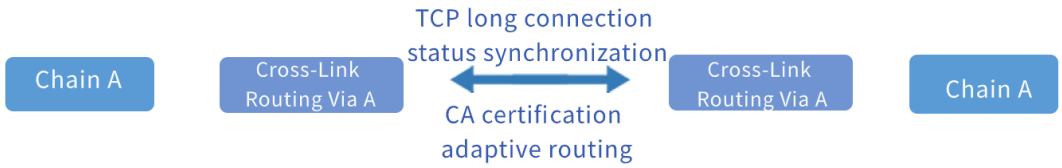
Cross-links need to establish connections between blockchains. In order to ensure that cross-links can maintain efficient, reliable and secure network connections, cross-links are designed with the following network mechanisms:

Network access: Cross-links support network access based on the CA authentication mechanism, support any number of levels of certificate formation, and ensure information confidentiality, authentication, integrity, and non-repudiation. All communication links use SSL encryption, and the encryption algorithm can be configured to ensure the security of data transmission.

TCP long connection: maintain long connections between links to ensure two-way communication and reduce the overhead of establishing and disconnecting connections. Cross-links use heartbeat packets between networks to ensure availability and automatically reconnect when disconnected.

State synchronization: Cross-links will automatically synchronize the state of the block height, consensus, and network of their respective blockchains.

Adaptive routing: Cross-link routing in a P2P network will automatically search for and confirm a feasible link with another cross-link routing, and evaluate the response speed, bandwidth and availability of the link, and automatically select the best link When a link fails, the cross link will select another available link to ensure the availability of side-chain messages.



D.3 Trusted transaction mechanism

As mentioned above about the design concept of Secure, based on the consensus mechanism and cryptography technology, the blockchain has established a set of internal security mechanisms, but when it comes to cross-blockchain scheduling, it will break through the security boundaries inside the blockchain and need to re-establish the security mechanism. Taking a blockchain platform based on the PBFT consensus mechanism as an example, all blockchain nodes participating in the consensus will not directly synchronize the state data from other nodes. Instead, download blocks from other nodes, verify the PBFT consensus signature in the block, then execute all transactions in the block, and update the status according to the execution result of the transaction data, to ensure that all data that needs to be chained is verified by signature checksum. However, in the cross-chain scenario, independent blockchain networks need to obtain data on each other's chains. Since they do not participate in the consensus process of each other's blockchain, how to ensure the credibility of the obtained data is a technical challenge.

Another technical challenge is to ensure the transactional execution of the respective on-chain transactions in cross-chain transactions, such as cross-chain asset transactions, so that all participating blockchains' operations on assets succeed or fail at the same time. In traditional distributed transactions, such as the transactions of multiple relational databases, multiple databases will choose a common trusted central coordinator to coordinate the transaction operations of multiple databases. The coordinator sends operation steps to multiple databases participating in the transaction, and monitors and manages the execution status of these operations. Once an exception occurs, the central coordinator will roll back the entire transaction and restore the system state. However, the status of multiple blockchain platforms in cross-chain scenarios is equal, it is difficult to choose a centralized coordinator, and it is not possible to implement distributed transactions in the traditional way.

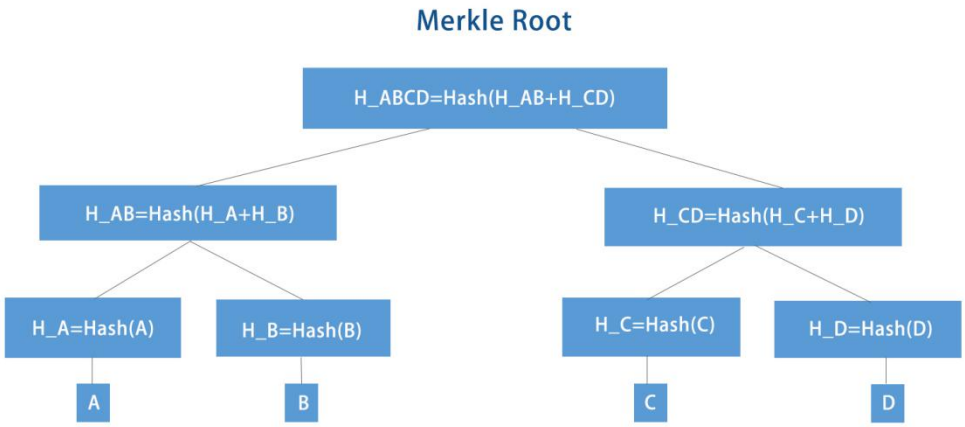
Another technical challenge is to ensure the transactional execution of the respective on-chain transactions in cross-chain transactions, such as cross-chain asset transactions, so that all participating blockchains' operations on assets succeed or fail at the same time. In traditional distributed transactions, such as the transactions of multiple relational databases, multiple databases will choose a common trusted central coordinator to coordinate the transaction operations of multiple databases. The coordinator sends operation steps to multiple databases participating in the transaction, and monitors and manages the execution status of these operations. Once an exception occurs, the central coordinator will roll back the entire transaction and restore the system state. However, the status of multiple blockchain platforms in cross-chain scenarios is equal, it is difficult to choose a centralized coordinator, and it is not possible to implement distributed transactions in the traditional way.

The purpose of the GMC Trusted Transaction Mechanism (TTM) is to solve the above-mentioned challenges, and propose a data mutual trust mechanism and a cross-chain transaction mechanism to solve the problem of data credibility and transactional issues, respectively.

D.3.1 Data mutual trust mechanism

Assume that two users A and B want to complete asset exchange on two different blockchains, then there must be a mechanism to ensure that both users truly own the claimed assets, otherwise users on either side can use the fake on-chain assets to exchange for each other's valid on-chain assets. The data mutual trust mechanism is to solve the problem of data credibility in this cross-chain scenario. It is implemented based on the Merkle proof mechanism, so that one party can quickly prove the true existence of specific data on the other party's blockchain without needing to obtain the full amount of data on the other party's blockchain.

The two parties involved in the cross-chain usually do not have the conditions and permissions to store the full amount of blockchain data of the other party. To verify whether a certain block contains a specific transaction without storing all the blocks, a special kind of data Structure—Mercury Tree is needed. The structure of the Merkel tree is shown in the following figure. Each non-leaf node is labeled by the hash value of its children. The root node of the tree shrew is called the Merkel root.



Assume the above figure is the Merkle Tree structure of block X. If you want to verify whether transaction D is in block X, you don't need to obtain the entire block X. You only need to provide transaction D, H_AB, H-C, and Merkle root. The specific process is as follows:

●Calculate a hash based on transaction D to get H_D.
●Calculate the hash according to H_C and H_D to get H_CD.
●Calculate the hash according to H_AB and H_CD to get H_ABCD.
●Compare H_ABCD and Merkel root. If they are the same, it proves that transaction X exists in block X, otherwise it means that it does not exist.

The above verification process is called Merkel proof, and the proof information refers to the initial hash values used in the verification process, namely H_ AB and H_C.

Merkle proof is a classic technology that is used to prove that a transaction exists in a certain block of the blockchain. It is a key technology for instant light clients. GMC uses Merkel's certification as the basic algorithm of cross-chain mutual trust technology. It has made a big step

forward in terms of functional completeness and user experience than traditional light clients, mainly in the following two aspects:

Multi-dimensional Merkel proof: GMC designs multi-dimensional Merkel proof, which can not only verify the existence of transactions, but also verify the correctness of transaction execution results, for the credible execution of cross-chain transactions and the transaction mechanism described in subsequent chapters Provide complete and trusted verification. Transaction existence verification refers to verifying whether a certain transaction really exists in a certain block and ensuring that the assets or data claimed by both parties in the cross-chain transaction are real. Transaction execution result correctness verification refers to verifying whether cross-chain transactions have been correctly executed on the respective blockchains of both parties to ensure the correctness of the results of cross-chain transaction executions. Among them, the existence of transactions requires the use of Merkel root transactions. The verification of the correctness of the results requires the receipt of Merkel root.

Completely transparent to users: The multi-dimensional Merkel mentioned above proves that the user is completely transparent in GMC, and the user's access to cross-chain resources is consistent with the experience of accessing resources within the chain. The cross-link component interaction layer contains a cross-chain certification module, which is responsible for implementing the Merkel proof mechanism. The user sends a cross-chain transaction request. The cross-link will find the business chain where the corresponding resource is located according to routing addressing. The cross-link will send the transaction to the business chain and obtain the relevant Merkel certificate. The certification data will be returned to the user along with the request result. The cross-link routing on the side and the cross-link routing on the user side verify the Merkel proof data. The whole process of data credible verification is performed by the cross-link and components, and the user does not need to care about the implementation details. With Merkel's proof mechanism, GMC can effectively verify the authenticity of cross-chain transactions and the authenticity of cross-chain transaction execution results, providing a basis for credible execution of cross-chain transactions. At the same time, the complex certification process is automatically implemented by cross-links and is completely transparent to users.

D.3.2 Cross-chain transaction machine drama

Also taking cross-chain asset exchange as an example, the mutual trust mechanism to ensure the authenticity and effectiveness of assets and transactions is still insufficient for the entire transaction process. Assume that the asset transfer is successfully completed on one chain, but the asset transfer is not successfully performed on the other chain, which will cause one party to lose assets and make cross-chain asset exchange failure. Although the data mutual trust mechanism ensures the credibility of cross-chain transactions, in order to perform cross-chain asset exchange completely and correctly, it is also necessary to ensure the transactionality of cross-chain transactions. The cross-chain transaction mechanism guarantees that all operations on multiple blockchains are completed or all executions fail. There are many traditional distributed system transaction technologies, such as two-phase commit and three-phase commit. They can achieve different levels of distributed consistency, each with its own advantages and disadvantages. In the early days of the blockchain, digital asset exchange was mainly used. Based on the particularity of

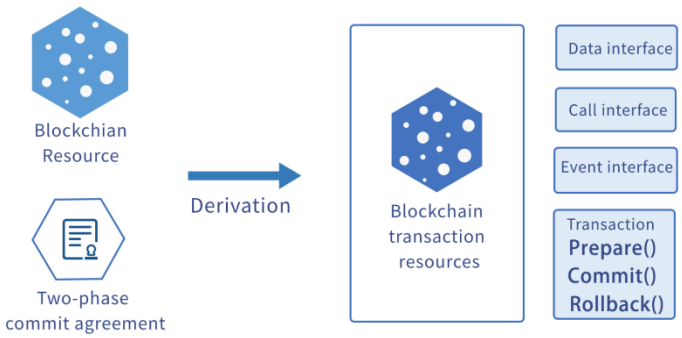
the blockchain architecture, there are also upgraded transaction technologies of the blockchain, including hash locking and distributed private key control. These technologies are mainly used to ensure cross- Transactionality in the chain asset exchange scenario. The goal of TTM is not only to support the exchange of cross-chain digital assets, but also to support more complex cross-chain scenarios, so it will gradually integrate and support existing mainstream transaction technologies, including two-phase commit protocols, hash-time locked contracts, and so on.

Two-phase commit agreement:

The two-phase commit protocol is an atomic commit protocol, designed to ensure consistency when processing transactions in a distributed system. The two-phase submission protocol has the advantages of strong reliability, universality, and simple implementation. Most services such as cross-chain transfers and cross-chain collaboration can be implemented using the two-phase submission protocol.

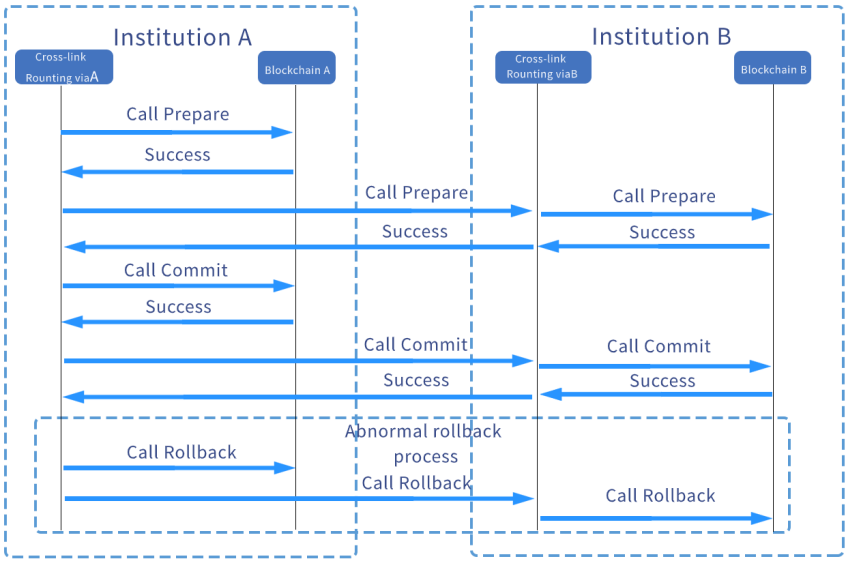
The two-phase commit protocol divides the transaction submission process into two phases, namely the voting phase and the commit phase. In order for the entire transaction to run normally, the two-phase commit protocol involves three interfaces, namely Prepare, Commit, and Rollback.

In the above "Uniform Resource Paradigm" chapter, a unified resource paradigm was introduced, defining three core interfaces for data acquisition, invocation, and event notification for resources. Combining the two-phase commit protocol, GMC adds three transaction interfaces to the resources that need to ensure cross-chain transactionality, as shown in the following figure.



In the "Cross-Chain Interaction Model" section above, the functional design of cross-link routing is explained, in which the transaction layer is responsible for implementing the cross-chain transaction mechanism. Cross-link will act as the coordinator in the two-phase commit protocol to coordinate the operation of the entire transaction. In the quasi-preparation phase, a cross-link will initiate a preparation request to all the resources involved in the transaction, and after all resources are prepared, a submission request will be sent to the whole body resource. In the two stages of preparation or submission, if any resource fails to return, the cross-link will initiate a rollback request to all the resources involved in the transaction, abandon the transaction, and restore the

original state. The cross-link integration process by the coordinated transaction mechanism is shown in the following figure.



The two-phase commit protocol has many advantages. Traditional databases and distributed systems use a large number of two-phase commit protocols to implement the transaction mechanism, so cross-chain transaction mechanisms also prefer the two-phase commit protocol.

The traditional two-phase commit protocol relies heavily on a reliable coordinator. If a malicious or abnormal coordinator intercepts or blocks some transaction requests, it will result in the interruption of the transaction process. The failure of the original cause will cause a single point of failure and the transaction cannot continue.

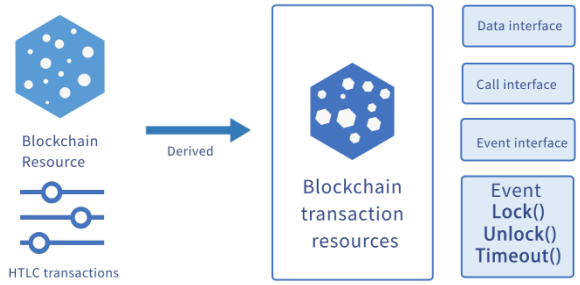
In order to avoid the above problems, TTM supports users to optionally build a blockchain dedicated to coordinating transactions outside multiple business blockchains, called a governance chain. The cross-links involved in transactions in each organization are connected to the governance chain through the configuration of a blockchain adapter. During the two-phase transaction process, the state of the transaction is recorded on the governance chain, so that the malicious coordinator cannot easily tamper with the two the status of the phase transaction. When the cross-links responsible for coordinating transactions are abnormal due to system or network reasons, other cross-links can obtain the transaction status from the governance chain, continue to process transactions, and avoid single-point problems.

Hash time locked contract

Hashed Time Lock Contract (HTLC) is a technology that exchanges assets between blockchain networks. In the process of asset exchange, in order to ensure the security of the assets of each blockchain, the asset transfer is either completed or not completed, and there is no intermediate state. Hash time lock contract is based on hash algorithm and timeout mechanism. Compared with

two-phase submission, HTLC does not rely on a trusted coordinator, which is especially suitable for blockchain asset exchange scenarios.

Based on the unified resource paradigm, the hash time lock contract adds three new interfaces to blockchain resources, namely the Lock, Unlock, and Timeout interfaces. As long as these three interfaces are correctly implemented, GMC cross-link can coordinate the blockchain resources and participate in any transaction that locks contracts based on hash time.



The processing process of a hash time lock contract is based on a hash algorithm and a timeout mechanism. Assuming there are two blockchains A and B, try to exchange assets a located on chain A and assets located on chain B. The entire hash time lock process as follows:

A first selects a secret random number S, uses a specific hash algorithm to calculate the hash value H of S, and then A sends H to B. At the same time, A and B negotiate two time points TO and TL to ensure T0> Tl.

A creates an asset-locking smart contract LockContractA based on H and TO. This smart contract will lock asset a. It can use S to unlock and transfer asset a to B. If it is not unlocked before TO, it will automatically revoke the lock determination, and No asset transfer will occur.

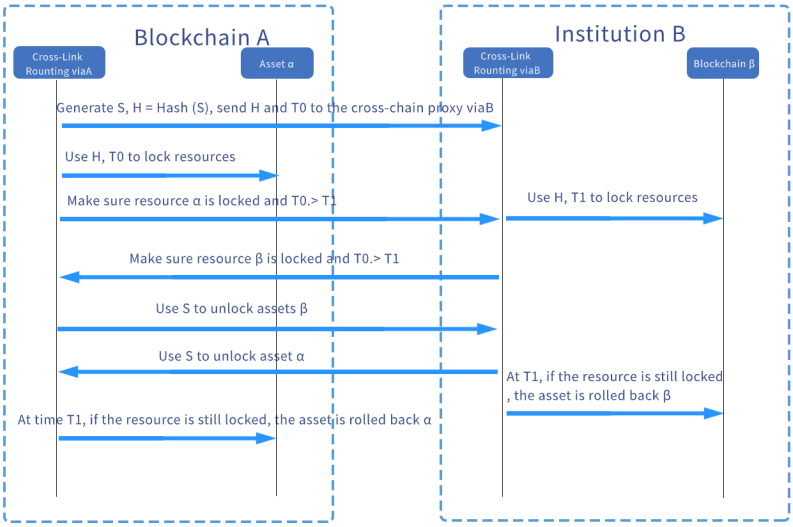
B creates an asset-locking smart contract LockContractB based on H and T1. This smart contract will lock the asset. Tian can use S to unlock and transfer asset 6 to A. If it is not unlocked before T1, the lock will be automatically revoked. No asset transfer will occur.

A uses the secret random number S to call LockContractB, the smart contract on B, to transfer the assets to A.

After the above steps, B obtains the secret random number S, and B uses S to call the smart contract LockContractA on A to transfer asset a to B, and the asset exchange is completed.

If either A or B does not perform the operation after the timeout, the asset B will be unlocked after the T1 time point, and the asset A will be unlocked and the original state will be restored after the TO time point.

TO and T1 are used to avoid A or B's unilateral delay in transactions. Therefore, both transaction package a and transaction package R need to set a time limit. After this time limit is exceeded, the relevant assets are immediately unlocked and returned to the original way.



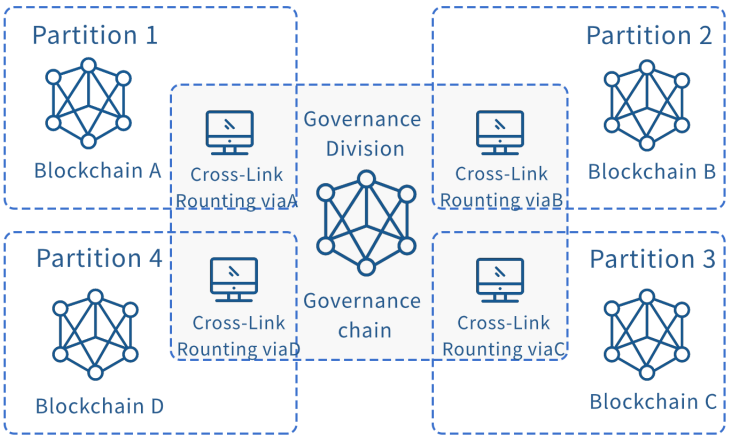
The two-phase commit protocol and hash-time-locked contract have their own characteristics. Two-phase submission can be used to satisfy general transaction processing requests, but it needs to rely on trusted coordinators. In order to introduce multi-center trusted coordinators, additional governance chains may be required to cooperate with the implementation. The hash time-locked contract does not rely on a trusted coordinator, which is suitable for the scenario of blockchain asset exchange. However, for scenarios other than asset / exchange, the process is more complicated and verbose, and there is no two-phase submission universal and effective.

D.4 Multilateral cross-domain governance

At present, the scalability bottlenecks faced by blockchains are becoming increasingly apparent. Some existing technical methods, such as multi-channel, multi-group, and multi-chain architecture, only solve the parallel expansion of blockchain capacity, but still lack credible access, supervision and governance mechanisms, so that cross-chain applications are limited to scenarios where participants are trusted.

Multilateral Cross-domain Governance (MIG) is a complete set of blockchain multilateral governance solutions that supports multiple blockchains to establish cross-chain partitions with different network topologies in accordance with their business and demand, and multiple institutions jointly maintain the governance chain to achieve multiple blockchains to execute transactions securely and reliably.

MIG conducts institutional access and blockchain governance through negotiation and voting, and supports immediate and effective regulatory arbitration.



A variety of smart contracts related to cross-chain governance are deployed on the governance chain, including rights management contracts, transaction management contracts, business chain supervision contracts, business chain access contracts, and institutional access contracts. These contracts focus on functions such as permissions, transactions, supervision, and access. The governance chain is jointly established by the relevant parties such as the business party and the regulator. Each institution can access the governance chain by configuring a blockchain adapter in its own cross-link router.

D.4.1 Rights transaction management

Resources on the blockchain may involve a variety of sensitive information such as personal assets, identity data, and business secrets. Reliable limit management and authorization mechanisms are required to ensure the information security of blockchain resources. By deploying permission management smart contracts on the governance chain, can refine the permission control of cross-chain operations to the specific interfaces of partitions, institutions, blockchains, and even resources. The cross-links of the access management chain are synchronized in real time and execute the permission policies from the rights management contract, control and record the resource access of cross-chain operations, and ensure the information security of cross-chain business in real time. The logic representation of the rights management contract is as follows:

Identification number (user or organization)	Resource path	Authority information
User or organization A	Asset resources pointing to the chain of evidence in the payment partition	Allows access to the data read interface
User or organization B	Asset resources pointing to the chain of evidence in the payment partition	Allows access to the data read / write interface
User or organization C	All resources pointing to all chains in the payment partition	Allow access to the call / transaction interface

Identification number: The identification number of the blockchain user or institution, as the primary key of the table, records the user or organization identification related to this permission entry.

Resource path: The resource path involved in this limit entry, iPath, supports wildcards.

Permission information: Control the resource interface that this permission allows to access, and any interface in the resource can be configured with independent permissions.

In addition to the control of permissions, cross-chain transaction operations are also scheduled through the governance chain. The governance chain deploys transaction management contracts to record the complete life cycle of transactions from generation to completion. The logical representation of the transaction management contract is as follows:

Transaction identification number	Step number	Step operation	Step status
0x100	1	Call the Prepared interface of resource a of blockchain A	Completed
0x100	2	Call the Prepared interface of resource b of blockchain B	Completed
0x101	1	Call the Commits interface of the resource y of blockchain A	Completed

Transaction identification number: A unique identification number for a transaction, which is generated every time a new transaction is created.

Step number: A transaction requires multiple steps to execute, and the step number is the number of the steps that a transaction has executed.

Step Action: The action required for this step.

Step status: The current status of the step.

The transaction management contract records the steps of the transaction on the governance chain and requires the consensus of all governance nodes. If an attacker tries to attack a transaction, maliciously tampering or discarding the transaction bag means that the attacker has to attack the governance chain maintained by multiple different institutions and tamper with the data on the chain, which is extremely costly. When the network or system fails, the current cross-links responsible for coordinating affairs cannot work, and other cross-links can continue the execution of transactions through the transaction steps recorded in the transaction management contract, thereby avoiding single-point problems to achieve the effect of disaster recovery.

D.4.2 Regulatory access management

The governance chain can selectively record some or all of the cross-chain operations between multiple cross-chain partitions for supervisory agencies to conduct penetrating supervision. Supervisors can choose to deploy a cross-link source that accesses the governance chain, or directly run a blockchain node of the governance chain to obtain regulatory data.

The regulatory data on the governance chain is stored in encrypted form and can only be decrypted and read by the regulator. Any malicious cross-chain operation in the cross-chain partition will be recorded in the governance chain for the supervisor to implement ex-ante interception, in-event monitoring, and post-accountability.

Business chain access contracts and institutional access contracts on the governance chain provide access control for businesses and institutions participating in cross-chain, and support the identification of business chains and institutions based on the CA certification mechanism. An organization's access contract can be configured with one or more administrators. The access information stored in the contract can be dynamically added, deleted, modified, and checked. When malicious behaviors occur in cross-chain partitions, administrators can initiate voting on the governance chain to punish or kick out malicious organizations.

The number of governance chains is not limited to one. In a complex network topology, multiple cross-chain partitions can form their own governance chains. Multiple governance chains are allowed to form higher-level governance chains to form a multi-level governance architecture. Each level of governance chain can directly manage the multiple governance chains it accesses, making it possible to build large-scale, cross-regional, massive data and manageable wide-area blockchain networks.

D.5 Consensus mechanism and security

As a global cross-industry interoperable collaboration platform created by blockchain technology, it is particularly critical to choose a set of efficient consensus mechanisms to ensure the normal and secure operation of the main chain in order to better reflect the design concept of the 5S principles.

D.5.1 Choice of consensus mechanism

The selection of the public chain consensus mechanism will consider the following factors: First, the consensus mechanism generally follows the CAP principle, namely Consistency, Availability, and Partition tolerance. It is difficult for the three to achieve the optimum at the same time. Second, when selecting and designing consensus, the basic nature of consensus needs to be considered:

Agreement: All honest nodes agree with a result;

Validity: The result of identification must be a valid one;

Termination: consensus must be reached within a certain period of time, not endlessly;

Combining theory with practice, GMC chose BFT-DPOS (Byzantine Fault Tolerance – Delegated Proof Of Stake) as the consensus mechanism. The specific considerations are as follows:

Compatible with all industry platform needs

GMC is a universal public chain platform for all industries in the world, and supporting the data on all industry platforms is the first goal to be achieved, so the availability of the system needs to be ranked first. In the CAP principle, the design of GMC needs to ensure system availability and partition fault tolerance, and appropriate compromises can be made for consistency. No guarantee is required for strong consistency, only the consistency of the results is required, and the characteristics of the BFT-DPOS mechanism are consistent with it.

High concurrent processing requirements

The main consensus mechanisms of existing blockchains are POW (Proof of Work, Proof of Work), POS (Proof of Stake, Proof of Share) and BFT-DPOS (Byzantine Fault Tolerance-Delegated Proof Of Stake). From the perspective of efficiency and energy efficiency, both the POW and POS mechanisms have significant problems at the design level.

The problems of the POW mechanism mainly exist in the centralization of computing power and energy consumption. On the one hand, the POW mechanism competes for computing power through the computing power of nodes. With the gradual upgrade of CPU mining to ASIC mining, there has been a trend of centralization of computing power, which conflicts with the concept of blockchain decentralization. On the other hand, POW wastes a lot of electric power to perform calculations. Bitcoin and Ethereum have always adopted the POW consensus mechanism in the early days.

The POS mechanism has improved in terms of energy consumption, but there are still hidden dangers in centralization. Specifically, there is a tendency for the POS mechanism to have more coins for people who hold more coins, and the entire network may become more and more centralized with the increase of the runtime. Therefore, although the POS mechanism saves energy compared to POW, the bottom layer still relies on POW, and it does not improve performance and security. Ethereum used the POS consensus mechanism at a later stage.

The DPOS mechanism is similar to the system for the election of the business meeting at the shareholder meeting, and the super node election mechanism is introduced. This design mechanism makes the block generation faster and more energy efficient. In addition, the DPOS mechanism makes full use of the votes of currency holders to reach consensus in a fair and democratic manner. The N super nodes elected by voting have equal rights, and the holders can change the super nodes by voting at any time. Although the DPOS mechanism still has centralization, this centralization is under control because each user has the right to decide which nodes can be trusted. The DPOS mechanism can theoretically achieve a transaction speed of million times per second. Under the condition of high network latency, it can reach the level of Lou 100,000 times per second, which is more suitable for enterprise-level applications. GMC, as a

public chain platform for all industries in the world, has extremely high requirements for data exchange and calculation and its stability in a trusted environment, so BFT-DPOS is a more suitable choice.

Demand for performance improvement

Although DPOS is relatively superior in performance over other consensus mechanisms, its performance is based on low faults and low latency. However, the current application scenarios are difficult to guarantee long-term low failure and low latency. Therefore, non-BFT DPOS mechanisms may have potential problems.

In the DPOS algorithm, block producers take turns to generate a block within a certain period of time. Assuming no node has stumbled its own round, the longest chain will be generated. It is invalid for block producers to produce blocks at any time other than the scheduled round. However, there may be cases where malicious encounters or faulty nodes create a small number of forks. In order to ensure that the chain where honest nodes are located becomes the longest chain, the number of honest nodes is required to account for more than 2/3 of the total. For example, there are three nodes A, B, and C, where A and C are honest nodes and B is a malicious node. It takes 2 seconds to generate a block under DPOS, so malicious node B can only generate one block every 6 seconds, and honest nodes can generate 2 blocks every 6 seconds, so the chain generated by an honest node is always more than the attack chain long. Similarly, consider other failure scenarios: such as dual production of a small number of offline nodes, network sharding, dual production of a small number of online nodes, insufficient legal super nodes, and fraud by most producers, all requiring the number of honest nodes to account for the total More than 2/3.

Therefore, under the traditional DPOS mechanism, in order to prevent forks and ensure the irreversibility of transactions, 2/3 ， of super nodes are required to confirm by continuing to produce blocks after the block. For example, there are 18 super-class nodes in the system, and one block is generated every 2 seconds. To achieve transaction irreversibility, it is necessary to continue to generate 12 regional blocks in the back, which takes 26 seconds (1 + 12 blocks).

In order to improve the performance of the GMC system, the BFT protocol can be introduced on the basis of the original DPOS, and the confirmation of the block signature is now completed when the block is generated, which shortens the time required for the transaction to be irreversible. Specifically, the super-level node packages the transaction into a block and signs the block with its private key, and broadcasts it to all nodes. When the super node receives at least 2/3 of the signature blocks of other super nodes, the block completes the verification of all nodes and becomes an irreversible block added to the blockchain. As each block is produced immediately after the production of a new block chain on the entire network, and the receipt of the old block confirmation can be carried out at the same time, therefore, from the generation of a block to becoming an irreversible block, the longest time required is only the time required for block generation plus the signature confirmation time of other super nodes, which only takes 3 seconds. Under the BFT-DPOS mechanism, the system's block generation interval is shortened, which reduces the delay of cross-chain communication. At the same time, the number of transactions that

can be confirmed per unit time is increased, which improves the overall performance of the blockchain system.

D.5.2 Blockchain security mechanism

Hash algorithm:

Cryptography is the foundation of blockchain. As a kind of asymmetric encryption algorithm in cryptography, the hash algorithm can transform an input of any length into a fixed-length output in a reasonable time, thereby ensuring that the information in the system cannot be tampered. In order for the hash function to achieve cryptographic applications, the following characteristics must be met:

A. Define a hash function Y = H (X);
B. For any input X, the length of H (X) is always the same;
C. The output value Y can be calculated based on the input value X, but the input value X cannot be calculated based on the output value Y;
D. The two input values X and X 'cannot be found and the output values H (X) and H (X') are equal;
E. Puzzle friendliness;

Among them, property C guarantees the confidentiality of the information. Property D guarantees that the hash function value is immutable.
If the information is tampered with, the entire hash value will be completely different. On the premise of the property CD, the property E can be derived
Puzzle-friendly. We set the output value to Y, the known input value M, and to find the unknown input value X of the puzzle so that Y = H (M || X) holds, the only way is to try all possible input values X. For example, Y is a 200-bit binary number. If brute force is used, all cases of Y include 2 ^ 200, and X is selected randomly. In the worst case, 2 ^ 200 hash operations are performed. In order to get a hash value that meets the requirements. The randomness of X is the best way to ensure the solution.

Account design:

Unlike the Bitcoin blockchain, GMC introduced the design of a multi-signature account model. Bitcoin does not have an account concept. The balance of each user is calculated from UTXO (the unspent transaction output) on the blockchain. All legal Bitcoin transactions can be traced back to the output of the previous transaction or transactions. The source of these chains are mining rewards, and the end is the transaction output that is not currently spent. All unspent output is UTXO for the entire Bitcoin network.

In the GMC system, each address corresponds to an independent account, and the global state is composed of a mapping between the account address and the account status, and the mapping is stored in the data structure of the Merkle tree. Because GMC has the concept of an account, it has real-time performance in the visual visualization of transactions and querying account status, and can view the current account status and transaction status in real time based on an account address.

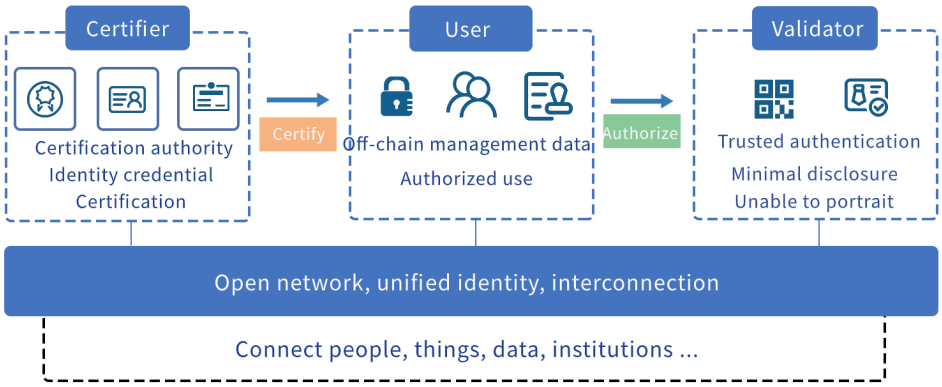
Digital signature:

Digital signatures are an important part of the blockchain, ensuring the security of the blockchain system. Digital signatures have two important characteristics. First, only the private key owner can sign the data, but any third party can use the public key to prove whether the data is valid. Second, the signature is only associated with a specific file, and the signature cannot be used to indicate that the owner supports a different file. The digital signature scheme consists of three algorithms:

(sk, pk) = generateKyes (keysize): The generateKeys method takes keysize as input to generate a pair of public and private keys. The private key sk is stored securely and used to sign the data. The public key pk is available to anyone and can be used to verify whether the signature is valid.

Sign = sig (sk, message): The signing process takes a set of data or message and a private key as an input, and the corresponding data or message is a signature.

isValid: = verify (sk, message, sign): The verification process takes a message and a signature and a public key as input. If the return result is true, the signature is valid, otherwise it is invalid.



At the same time, the following two properties are required:

A. A valid signature can be verified: Verify (pk, message, sign (sk, message)) === true.

B. The signature cannot be forged.

E. GMC Release Notes

At present, the application of blockchain technology is trying to issue tokens as a tool for economic incentives to promote the collaboration of various roles in the ecosystem. Therefore, every blockchain project based on token incentives is trying to design a token-based economic system that works well. However, even the best projects can hardly design a perfect economic model. Because in the digital world of the blockchain, the token economic model needs to be able to fully reflect the value of the real world and achieve accurate model fitting based on changes in the real world. However, this vision is difficult to achieve because there are too many variables to consider, which makes the token economy of many projects extremely unstable, and ultimately ends in failure.If the token economy system based on the blockchain technology is regarded as a miniature and perfect economic system, the formulators of the system rules need to conduct macro-control by controlling output channels, speed, and quantity.

If the token economy system based on the blockchain technology is regarded as a miniature and perfect economic system, the formulators of the system rules need to conduct macro-control by controlling output channels, speed, and quantity.

Based on various considerations, the GMC platform decided to adopt a balanced deflation model to build a platform ecology. Equilibrium deflation can greatly simplify the interaction between the system platform and users, effectively realize the resource separation of the right of use and equity, so that the platform business is not affected by external economic fluctuations, and ensure that the platform can operate continuously, stable and healthy.

E.1 Issuing mechanism

Issuing model: Determine the deflation model.

Total issued amount: 100000000 (1 billion)

Consensus mechanism: BFT-DPOS.

Block production time: 3 seconds.

E.2 Release plan

The release of TCP represents the beginning of an era, opening up the value exchange of the global general industry, opening up the island of trust between platforms, and realizing a new situation of value sharing and win-win cooperation in a true sense. Once issued, TCP will never be issued again. In order to reflect its value and determine the true meaning of the deflation model, GMC plans and allocates plans in smart contracts when issuing TCP as follows:

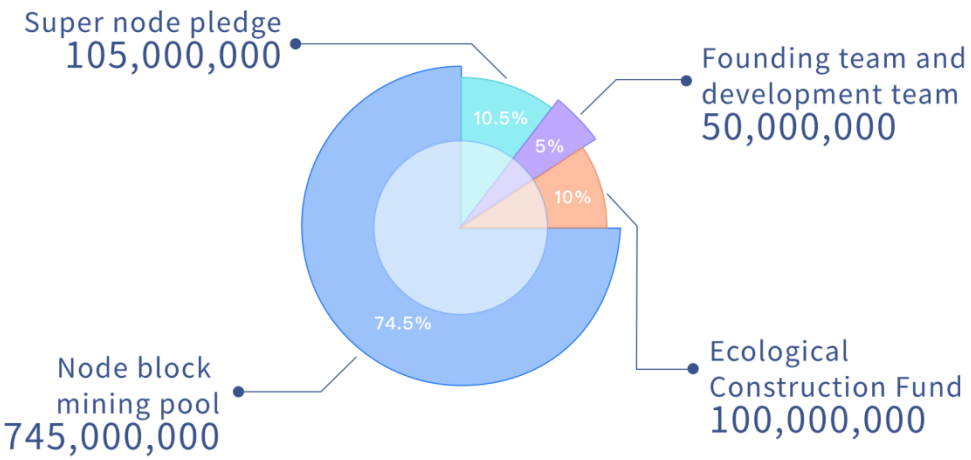
Super node pledge: As 21 super nodes to ensure the stable operation of the GMC platform, each super node needs to pledge 5000000 (5 million) for voting, for a total of 105000000 (105 million).

Founding team and development team: 50 million (50 million) pre-mined for initial ecological construction and later technical maintenance.

Ecological construction fund: Pre-mining 100 million (100 million) late-stage ecological construction. The late-stage ecology includes global commercial collaborative links, cross-platform advertising of ads, decentralized encrypted chat, etc. Please refer to the GMC ecological description below for details.

Node block mining pool: 745000000 (740 million), all users and platforms participating in GMC are independent nodes, and each node will form a block mining pool in the corresponding node after the completion of building and hosting. The mining pool will have a certain amount of TCP, and the TCP in the block mining pool will become the only value circulation and exchange for users on the platform.

Destruction mechanism: The destruction mechanism of traditional tokens basically adopts the repurchase method, and then uniformly destroys them. This method is manual operation and does not meet the decentralized thinking. GMC pioneered the use of multiple destruction mechanisms in the destruction mechanism. Smart contracts will implement different destruction strategies based on different behaviors on the chain, thereby achieving long-term deflation. It is estimated that 20% of the circulation will be permanently destroyed every month, and the total destruction will be 70% of the circulation.



F、GMC Ecology

As blockchain sparks spread around the world, and technology has become increasingly complex over time, one of the latest buzzwords in the technology industry is "ecosystems," especially "blockchain ecosystems." The concept of ecosystem is derived from biological terms used to describe the interaction of biological communities and their relationship with their environment. Nowadays, this analogy has extended to the blockchain world, where the ecosystem involves different participants, including interactions between participants, decentralized applications with the blockchain, and relationships with the external real world.

F.1 Global Business Collaboration Link

The Internet has spawned a global online business model, and numerous online merchants and online shopping groups have also been born, but this traditional Internet + business can never solve problems such as trust, privacy, and security. As the blockchain technology is gradually becoming familiar, more and more people are considering how to enable business to apply the blockchain technology, and use the blockchain to take advantage of inherently distributed, anonymous, and encrypted technologies to solve many problems that the traditional Internet cannot solve. So far this idea has remained at the stage of thinking.

So why are few people using and experiencing blockchain applications in real life? The GMC team found that there are two main reasons. One is the lack of hard enough real needs. People have become accustomed to the current Internet applications. This kind of inertia rooted in thinking has made the emergence of killer applications difficult. Second, there is not enough convenient user experience. When users use blockchain applications, they need to know about cryptocurrencies, keys, wallets and other related knowledge in advance, and the market education threshold is too high.

For example, if you want to make a social application software on the blockchain, the user's behavior on the software will be measured and stimulated with coin reward in the form of cryptocurrencies, such as likes, comments, and reposts. But at this time there is a very difficult problem. In the traditional blockchain application model, these on-chain behaviors require users to pay a fee to confirm the operation, which will bring a very awkward scene. Users pay a certain amount of cryptocurrency each time they post or repost on the software.

In fact, the user will not be willing to pay this money, because he has not thoroughly understood the principles of blockchain and cryptocurrency. Node service provider). Users will not have the motivation to experience a new software, recharge to buy cryptocurrencies with high volatility as a payment method. In short, this not only violates the current habits of Internet users, but also makes users have to understand the operating principles behind blockchain and cryptocurrencies. It also violates human nature. Good products should be subject to the "lazy" Human nature.

The GMC technical team has fully considered the above factors when designing the bottom layer, and for the first time proposed a relay node (Replay) fee payment mechanism, and also designed

two types of payment mechanism protocols: multi-party payment protocol (MPP) and designated payment protocol VIP-191).

The Multiparty Payment Protocol (MPP) allows an account on a chain to pay transaction fees for transactions sent from a specified account to that account. MPP is mainly aimed at DApp owners who have multiple contract accounts on the chain. In the agreement, only DApp owners can set up MPPs for their contracts. Since MPP needs to record related information on the chain, it will incur some indirect costs. Therefore, from a cost perspective, the MPP protocol is more suitable for scenarios where the user and the DApp have a relatively stable relationship.
The designated payment agreement (VIP-191) is a supplement to the Multi-Party Payment Protocol (MPP), which provides greater flexibility for transaction fee payment on VeChain. VIP-191 allows transaction senders to find any fee payment party. It does not have to be the owner of the contract to which the transaction is directed. In other words, the user does not necessarily choose the DApp or application project party to pay the miner fee, but has a variety of options.

The GMC technical team has fully considered the above factors when designing the bottom layer, and for the first time proposed a relay node (Replay) fee payment mechanism, and also designed two types of payment mechanism protocols: multi-party payment protocol (MPP) and designated payment protocol VIP-191).

The Multiparty Payment Protocol (MPP) allows an account on a chain to pay transaction fees for transactions sent from a specified account to that account. MPP is mainly aimed at DApp owners who have multiple contract accounts on the chain. In the agreement, only DApp owners can set up MPPs for their contracts. Since MPP needs to record related information on the chain, it will incur some indirect costs. Therefore, from a cost perspective, the MPP protocol is more suitable for scenarios where the user and the DApp have a relatively stable relationship.
The designated payment agreement (VIP-191) is a supplement to the Multi-Party Payment Protocol (MPP), which provides greater flexibility for transaction fee payment on VeChain. VIP-191 allows transaction senders to find any fee payment party. It does not have to be the owner of the contract to which the transaction is directed. In other words, the user does not necessarily choose the DApp or application project party to pay the miner fee, but has a variety of options.

GMC's two types of payment mechanism agreements give third-party developers more choices based on their user groups and usage scenarios. At the same time, the barriers between shopping platforms can be broken to truly realize information exchange and asset circulation. Connect more mall rights and scene rights, fully activate the "sleeping" shopping mall, build a digital shopping mall business ecological alliance, and achieve a win-win situation for the industry, business, and consumers.

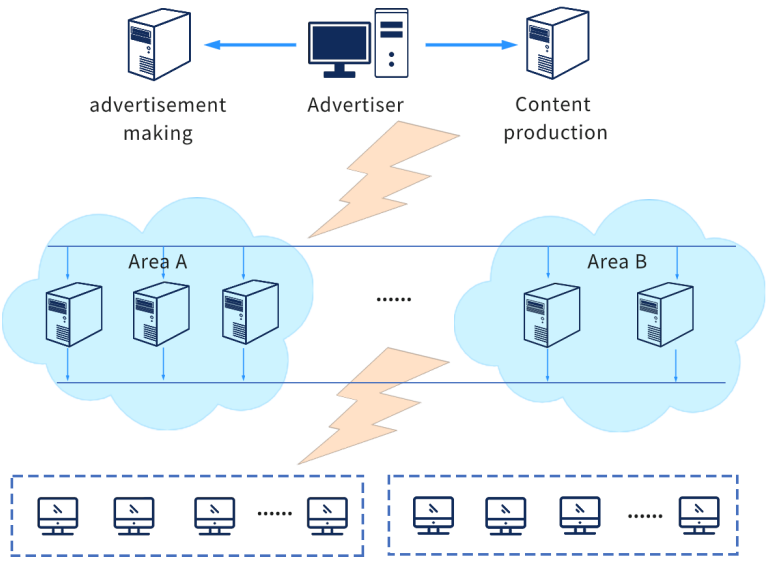
F.2 Advertising cross platform

Today, our lives are full of digital information. Especially in an open business environment, we can always receive countless advertising messages at various time and places. The powerful market behind this phenomenon is the powerful demand.

Digital signage technology is also rapidly developing based on the evolving information receiving medium. Due to the advantages of paperlessness and fast content updates, people have begun to get used to obtaining information via digital media, replacing traditional static notice advertisements. We are more convinced that the advantages brought by digital media will not only be limited to new media presentation methods, but even more, we will provide various forms of digital media services for the purpose of the enterprise and interact with what people see and think.

In this era, people have more and more channels to obtain information, and the forms of advertising and information release have also changed from traditional text and pictures to multimedia information. More and more advertisers are beginning to change their mindset, that is, to expand the scope of coverage, and also to quickly and accurately deliver information to the corresponding target customer base. Reasonable and effective advertising can not only improve the overall image of enterprises and institutions, but also provide users with timely, comprehensive and rich information, reflecting the concept of efficient and high-quality services.

GMC placed the decentralized advertising cross-platform application in an important position when designing the global business platform, and specially designed a set of decentralized multimedia information publishing system, referred to as De-ADS. De-ADS allows enterprises, large institutions, operators, or chain-based institutions to publish a variety of media information such as videos, pictures, subtitles, Flash animations, web pages, slides (PPT), etc on the GMC platform and push them to terminal nodes in a timely manner to provide users with high-quality multimedia information service.

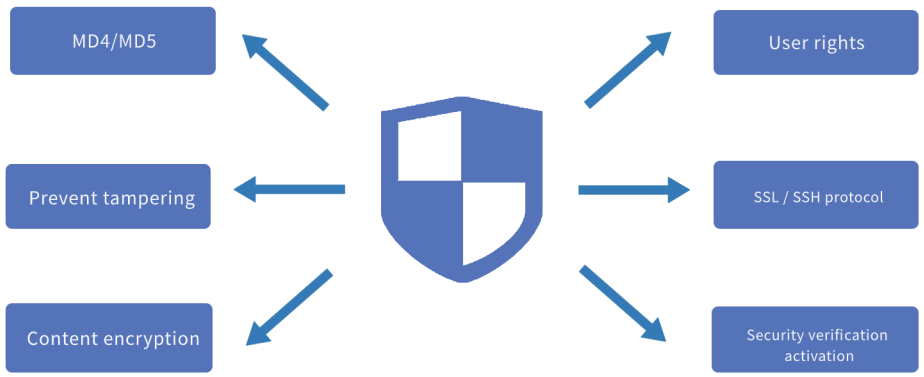


The goal of De-ADS is to provide users with convenient and fast operation, a powerful management platform, a stable, secure, and scalable system. Decentralized advertising distribution

is implemented in a decentralized manner. The distribution service provides precise advertising by region, region, and time period. The advertising content is automatically filtered and filtered before delivery, so as to provide advertising audiences and advertising demand parties with the best Quality advertising content services.

De-ADS has fully solidified the security mechanism:

- ⬤Advertisers use independent permission encryption management to ensure that the system uses a clear hierarchy and clear permissions.
- ⬤Network transmission link security, supports SSL protocol, and encrypts transmitted data to ensure the safe arrival of data.
- ⬤Integrity verification of published content, verify the integrity of published content through MD4 / MD5.
- ⬤Through the automatic feedback method of terminal nodes, the effectiveness of the published content effect is guaranteed and the advertising content is prevented from being tampered with.
- ⬤Encryption of published content. During content release, terminal theft prevents copying, copying, and modification of content.
- ⬤SSH connection and configuration services.



F.3 Decentralized encrypted chat

As technology barriers are overcome and landing applications mature, the blockchain will be increasingly applied to a variety of diverse scenarios. It may not be enough just to change the business model. But if the blockchain can make people's lives more convenient, and create a dream society that combines technological advancement and the pursuit of more idealization, people will look forward to this day.

Although the traditional Internet communication industry has developed to this day, although a relatively complete system has been formed, people still have higher expectations and demands for communication. In the era of centralized processors dominating Internet communications,

more people are worried about the privacy and security of personal information, calling for a more convenient user experience and more reliable communication channels.

GMC has carried out effective technical integration on the point-to-point information transmission and information encryption in the field of instant messaging. It has the characteristics of high reliability, privacy, and secure transmission. There is no central server to store data, and the information is sent anonymously, which is of great value in both personal communications and commercial applications.

How to achieve secure communication?

Through the point-to-point transmission protocol, a single node is used to replace the centralized server, and user information and configuration information will be distributed on the blockchain network. All communications on the protocol will use a trusted peer-to-peer encryption standard. Private keys will be used for encryption and decryption. Data is highly confidential and no third party can steal information.

Public key type:

- Identity Key Pair: A long-term Curve25519 key pair, generated during installation.
- Signed Pre Key: A mid-term Curve25519 key pair, generated during installation, signed by the identity key, and periodically rotated.
- One-Time Pre Keys: One-time use of the Curve25519 key pair queue, generated during installation and replenished when insufficient.

Session key type:

- Root Key: A 32-byte value used to create a chain key.
- Chain Key: A 32-byte value used to create a message key.
- Message Key: 80-byte value, used to encrypt the message content. 32 bytes are used for the AES-256 key, 32 bytes are used for the HMAC-SHA256 key, and 16 bytes are used for the IV.

Session initialization settings

Before you start a chat, you need to establish an encrypted session. Once an encrypted session is created, you do not need to repeat the session unless the session fails (such as reinstalling applications or replacing devices).

Establish a session:

The session initiator applies for the recipient's public identity key (public identity key), signed pre-shared public key (public signed pre key), and one-time pre-shared key (one-time pre key).

The server returns the requested public key. The One-Time Pre Key is used only once, so it will be deleted from the server after the request is completed. If the One-Time Pre Key is used up and has not been replenished, it returns null.

- The initiator saves the recipient 's Identity Key as Irecipient, the signed Pre-shared key (Signed Pre Key) as Srecipient, and the one-time pre-shared key (One-Time Pre Key) as Orecipient.
- The initiator generates a temporary Curve25519 key pair-Einitiator
- The initiator loads his own Identity Key as an Iinitiator
- The initiator calculates the master key: master_secret = ECDH (Iinitiator, Srecipient) || ECDH (Einitiator, Irecipient) || ECDH (Einitiator, Srecipient) || ECDH (Einitiator, Orecipient). If there is no One-Time Pre Key, ECDH will eventually be ignored.
- The initiator uses the HKDF algorithm to create a root key and a chain key from the master_secret.

Receive session:

After establishing a long-term encrypted session, the initiator can immediately send a message to the recipient, even if the recipient is processing offline. Before the receiver responds, all messages from the initiator will contain the information needed to create the session (in the message header). This includes the initiator's Einitiator and Iinitiator. When the receiver receives a message containing the session settings:

- The recipient uses his private key and the public key in the message header to calculate the corresponding master key
- Recipient deletes One-Time Pre Key used by initiator
- The initiator uses HKDF algorithm to derive the corresponding Root Key and Chain Keys from the master key.

Exchange messages

Once the session is established, clients are exchanged messages protected by AES256 message key encryption (CbC mode) and HMAC-SHA256 authentication.

The message key is transient and changes after each message is sent, so that the message key used to encrypt the message cannot be reconstructed from the sent or received session state.

The message key is derived from the "ratchets" forward of the sender's Chain Key when sending a message. In addition, a new ECDH protocol is executed for each message tour to create a new chain key. Provides forward security by combining an instant “hash ratchet” and a touring “DH ratchet”.

Calculate Message Key by Chain Key

Each time a message sender needs a new message key, the calculation is as follows:

- Message Key = HMAC-SHA256 (Chain Key, 0x01)
- The Chain Key was subsequently updated to: Chain Key = HMAC-SHA256 (Chain Key, 0x02)

This forms a forward "ratchets" chain key, which also means that the current or past chain key value cannot be derived using the stored message key.

Calculate Chain Key from Root Key

Each message sent is accompanied by a short-term Curve25519 public key. Once the response is received, the new Chain Key is calculated as follows:

- ephemeral_secret = ECDH (Ephemeralsender, Ephemeralrecipient)
- Chain Key, Root Key = HKDF (Root Key, ephemeral_secret)

A chain key can only send messages to one user, so the message key cannot be reused. Due to the calculation of message keys and chain keys, messages may be delayed, out of order, or completely lost without problems.

Transmission media and attachments

Any type of large attachment (video, audio, image or file) is also encrypted end-to-end:

- The sender generates a 32-byte AES256 temporary key and a 32-byte HMAC-SHA256 temporary key.
- The sender encrypts the attachment with AES256 key (CBC mode) and random IV, and then attaches the MAC using HMAC-SHA256 ciphertext.
- The sender uploads the encrypted attachment to the server for binary storage.
- The sender sends an encrypted message to the recipient containing the encryption key, HMAC key, SHA256 hash of the encrypted binary, and a pointer to the binary storage
- The recipient decrypts the message, retrieves the encrypted binary data from the server, verifies the AES256 hash, verifies the MAC, and decrypts it into plain text.

Group message

Traditional unencrypted chat applications usually use "server-side fan-out" for group messages to send group messages. When a user sends a message to a group, the server distributes the message to each group member. The "client-side fan-out" is the client sending messages to each group member. GMC's group messages are built on the paired encrypted sessions listed above to efficiently implement a large number of group messages through server-side fan-out. This is done through the "Sender Keys" of the Signal Messaging Protocol.

Group members send messages to the group for the first time:

- The sender generates a random 32-byte chain key.
- The sender generates a random Curve25519 signing key pair.
- The sender combines the 32-bit chain key (Chain Key) and the public key in the signature key into a message sender key (Sender Key).
- The sender uses a pairwise transmission protocol to individually encrypt the sender keys (Sender Keys) for each group member.

All subsequent messages to this group:

- The sender obtains the Message Key from the Chain Key and updates the Chain Key
- The sender uses AES256 to encrypt the message in CbC mode
- The sender signs the ciphertext with a Signature Key
- The sender sends a single ciphertext message to the server, and the server distributes the message to all group members

The "hash ratchet" of the sender's Chain Key provides forward security. When the group members leave, all remaining group members clear the Sender Key and regenerate.

Call settings: GMC is also end-to-end encrypted for voice and video calls. When a user initiates a voice or video call:

- The initiator establishes an encrypted session with the receiver (if not already established)
- The initiator generates a random 32-byte secure real-time transfer protocol (SRTP) master secret
- The initiator sends an encrypted message to the receiver containing the Secure Real-Time Transport Protocol (SRTP) master key for signaling
- If the call is answered, then a Secure Real-Time Transport Protocol (SRTP) call is initiated

Status

State encryption is very similar to group messages. Sending the first status to a specified group of recipients follows the same steps as sending a message to the group for the first time. Similarly, sending subsequent statuses to the same group of recipients follows the same steps as sending group messages. When the status sender changes the status privacy setting or deletes the number from the address book to delete the recipient, the status sender clears the sender key and regenerates it.

Authentication key

Users can also verify the keys of the users they communicate with so they can confirm that an unauthorized third party has not launched a man-in-the-middle attack. This can be done by scanning a QR code or by comparing 60 digits. The QR code includes:

- version number
- User identity on both sides
- Full 32-byte identity public key for both parties

When a user scans the other party ’s QR code, the keys are compared to ensure that the identity key in the QR code matches the one retrieved by the server. Calculate a 60-digit number by stitching the 30-digit fingerprint of two user identity keys. To calculate a 30-digit fingerprint:

- Repeat the SHA-512 hashed identity public key and user identifier 5200 times
- Get the first 30 bytes of the last output hash
- Divide 30 bytes into 6 groups of 5 byte data blocks
- By parsing each group of 5-byte data blocks into big-endian unsigned integers and modulo 100,000 times into 5 numbers
- Connect six groups of 5 numbers each into 30 digits

Transmission security

All communication between the client and server is layered within a separate encrypted channel. These end-to-end encryption clients can use Noise Pipes and use Curve25519, AES-GCM, and

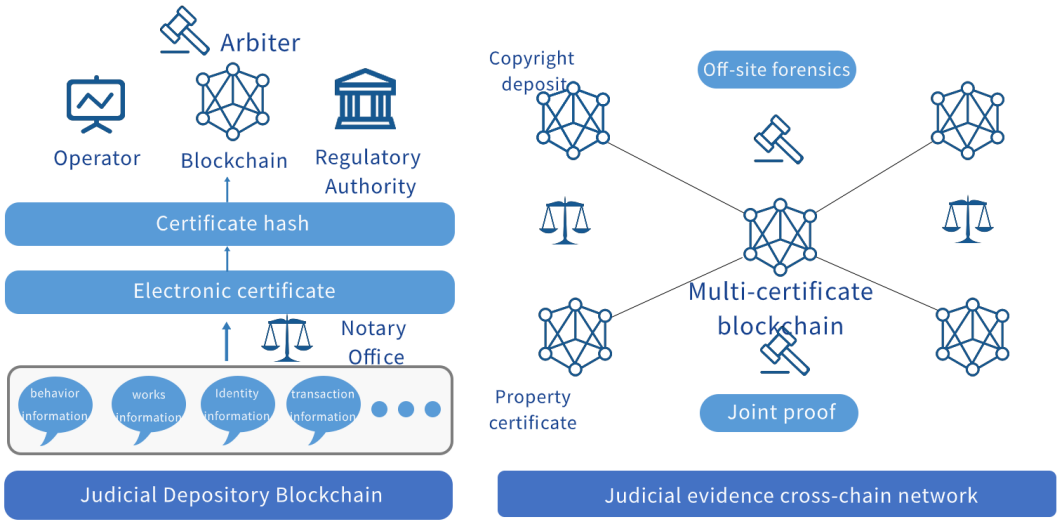
SHA256 in the Noise Protocol Framework to implement long-term interactive connections. This gives the client some nice properties:

- Extremely fast lightweight connection setup and recovery
- Encrypt hidden metadata to prevent unauthorized network listening. No information about the identity of the connected user was disclosed.
- The client's security authentication information is not stored on the server. The client uses the Curve25519 key for authentication, so the server only holds the client authentication public key (public authentication key). If the server's user database is compromised, personal authentication credentials will not be revealed.

F.4 Judicial cross-domain arbitration

With the rapid development of the digital economy, judicial evidence is gradually entering the electronic age. GMC proposed a blockchain judicial deposit and arbitration platform, and pioneered the concept of using arbitration, courts and other institutions as nodes on the chain. As the judicial application of blockchain can greatly reduce the arbitration process, arbitration institutions can quickly complete evidence verification and quickly solve the disputes.

With the popularity of blockchain applications in the field of judicial evidence, the need for connectivity between different judicial evidence chains has become stronger. However, the blockchain's trust model makes it impossible for the evidence on different judicial depositary chains to communicate and trust each other. When judicial arbitration requires remote evidence collection or joint proof, it is necessary to introduce a centralized trusted institution for coordination, which affects the practical value of the blockchain.



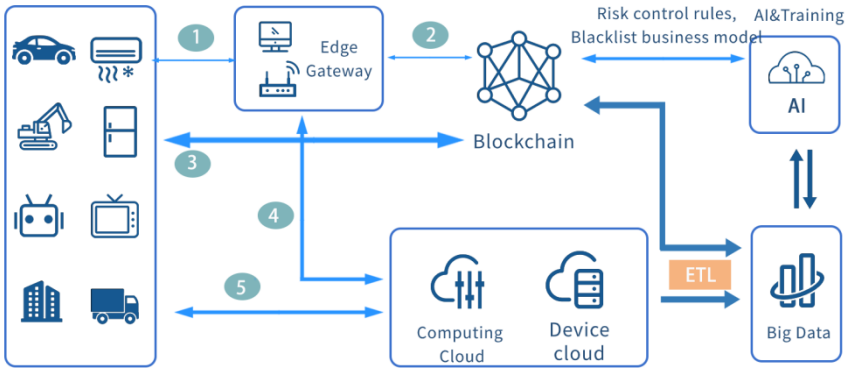
GMC cross-chain technology can uniformly abstract the evidence of each evidence chain into evidence resources, and credibly transfer evidence between different judicial evidence chains. GMC can build a network of certificate deposit chains with multiple types of certificate deposits. When facing major problems and major disputes, it can help each chain interact with complete, credible and legally valid evidence materials, and help arbitration institutions complete their awards.

F.5 IoT cross-platform linkage

With the popularization of artificial intelligence devices such as smart wear-and-tear, smart home, drones, and face recognition, there are more and more types of smart devices, and the frequency of human-computer interactions is getting higher and higher, and the types of IoT data and the structure shows a trend of diversification and complexity. In the 5G era, after the interconnection

of all things, the complexity of data and scenes has increased geometrically. Blockchain technology provides a trust mechanism for IoT devices to ensure the credibility, reliability, and transparency of records such as ownership and transactions. At the same time, it can also provide a guarantee mechanism for user privacy, thereby effectively solving the problems of big data management, trust, security and privacy faced by the development of the Internet of Things, and promoting the evolution of the Internet of Things to a more flexible and intelligent form.

At present, some blockchain projects in the IoT industry are aimed at solving the pain points of the severe fragmentation of the Internet of Things and the lack of standardization of IoT products, while others explore the blockchain in smart cities, infrastructure, smart grids, supply chains, and rhenium applications in transportation and other fields. However, they all face the same dilemma. The choice and combination of hardware modules for IoT devices is very diverse, and their support capabilities for regional blockchain platforms are not the same. Once the hardware deployment is difficult to update, a single blockchain platform will inevitably encounter a bottleneck when connecting multiple IoT devices, and cannot fully meet the needs of all IoT devices in diverse scenarios.



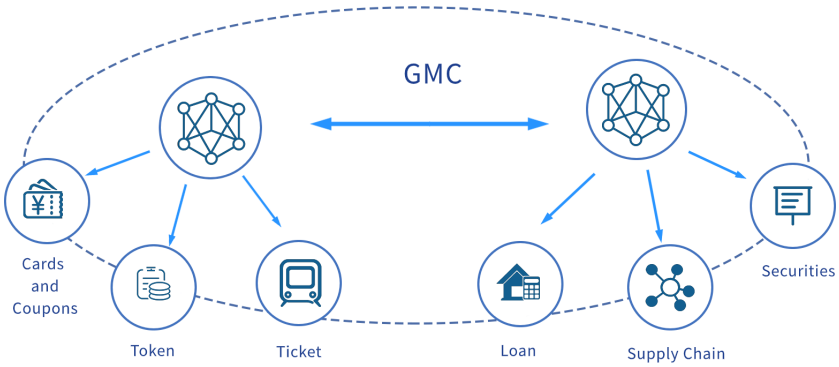
GMC cross-chain technology supports the parallel expansion of IoT devices across chains. It can be used to build efficient and secure distributed IoT networks and deploy data-intensive applications running on massive device networks. GMC cross-chain technology can securely and credibly integrate the blockchain that connects multiple IoT devices, and meets the needs of various scenarios in terms of functionality and security.

F.6 Digital asset exchange

Blockchain naturally has financial attributes and is expected to bring more innovation to the financial industry. In terms of payment and settlement, under the framework of blockchain-based technology, multiple ledgers or blockchains maintained by multiple participants in the market are integrated, connected and interact in real time.In just a few minutes, payment, reconciliation, and settlement tasks that can be completed in just two or three days can be completed, reducing the complexity and cost of cross-border transactions.cross-banking. At the same time, blockchain technology can ensure that transaction records are transparent and secure, and it is convenient for regulators to track transactions on the chain and quickly determine the flow of high-risk

transactions. In terms of digital bills and supply chain finance, blockchain technology can effectively solve the problem of financing difficulties for SMEs. The current supply chain finance is difficult to benefit small and medium-sized enterprises in the upstream of the industrial chain, because they often do not directly trade with core companies, and financial institutions have difficulty assessing their credit qualifications. Based on blockchain technology, an alliance multi-chain network can be established, covering core enterprises, upstream and downstream suppliers, financial institutions, etc. Core enterprises issue receivables vouchers to their suppliers. After the digitalization of the bills, they can be used by suppliers Cross-chain circulation between suppliers, each level of suppliers can use digital bills to achieve the corresponding amount of financing.

With the rapid growth of the application of blockchain in the financial field, the diversified digital asset scenarios and blockchain applications have brought about the issue of the isolation of blockchain assets. Different digital asset businesses on the blockchain built by each other Digital assets cannot be securely and reliably interoperable. The value of digital assets existing on the blockchain is getting greater and greater, and the need for cross-chain is increasingly urgent.

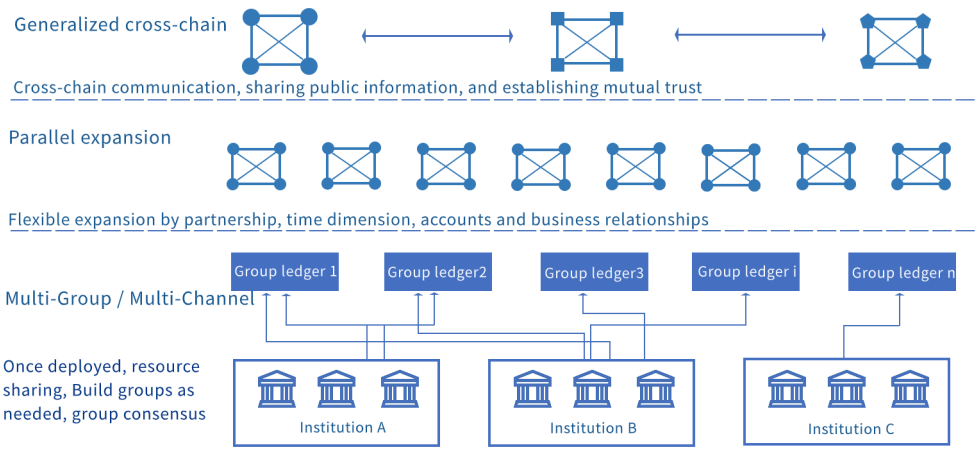


GMC supports cross-chain partitioning of digital assets with multiple network topology models. In terms of transaction logic, the two-phase transaction model and the HTLC transaction model will realize the decentralization, detrust, and immutable transfer of digital assets. In terms of security protection, encryption and access mechanisms will ensure the security and credibility of digital asset transfers. Through the above technical advantages, GMC will help to fully digitize asset certificates in the past in paper form, allowing assets and credits to be passed to the end of the industrial chain, and promote the development of the digital economy.

G、Outlook

As a forward-looking emerging technology, blockchain has attracted much attention, and a new wave of science and technology has emerged worldwide. With the acceleration of the application of the blockchain industry, the blockchain has gradually penetrated and spread from the financial industry to the non-financial industry. It has played an important role in many fields such as judicial depository, Internet of Things, intelligent manufacturing, and identity management, which has led to diversified technical solutions program. In the future, if the application of blockchain is going from single to multiple, it will inevitably face more complex scenarios, more participants, more prominent data islands, and the dilemma of achieving interconnectivity is of great significance.

GMC proposes the 5S cross-chain design concept in view of the status and problems of the blockchain industry. GGC designs a universal, efficient, secure and scalable blockchain cross-chain collaboration platform to achieve interoperability, mutual recognition, interconnection, mutual trust, and mutual visits between mainstream blockchain platforms. GMC highly abstracts the blockchain system and cross-chain network architecture, reduces the cost for users to deploy and use the blockchain, and proposes four core technologies to solve key blockchain abstractions in cross-chain scenarios, different temple chain interconnection, trust issues and multilateral governance issues. GMC is not only oriented to specific concrete application scenarios such as digital asset exchange, judicial arbitration, and the Internet of Things, but also will serve as the infrastructure for future distributed commercial blockchain interconnection, promoting cross-blockchain value exchange and commercial cooperation across industries, institutions, and regions to achieve an efficient, universal, and secure blockchain cross-chain collaboration mechanism.



It is foreseeable that the multi-chain architecture of the blockchain will undergo multi-group, multi-channel, parallel expansion, and eventually evolve to a generalized cross-chain architecture based on GMC, integrating and connecting a large number of blockchain platforms, whether homogeneous or heterogeneous. GMC will help the blockchain technology to make new breakthroughs in the diversity of business and network topology, and form a hierarchical and deep

cross-chain collaboration, so as to promote the combination of blockchain with emerging technology industries and traditional industries to create " Blockchain + "new business model.

At the same time, we position GMC as a "common language" between chains, adhering to the spirit of "seeking common ground while reserving differences" and "building together". At the technical and application level, we all strive to establish open and extensive cooperation with the industry. GMC's solutions and code are completely open source and continuously updated. More people are welcome to participate in the open source community contributions, platform docking, and application practices. The more people participate in cross-chain research and application, the more feasible the cross-chain solution is, the more feasible and sustainable it is. Such "network scale benefits" are not only reflected in the chain, but also can span scenes, regions, and crowds to accommodate greater value.

Looking forward to the future, the GMC blockchain team will, as always, not forget the original intention, focus on the current status and trends of cross-chain technology development, improve the ability to use and manage cross-chain technology, and enable cross-chain technology to help build a network country, develop a digital economy, and help the economy Play a greater role in social development and other aspects.