2024 全球6G技术大会
GLOBAL 6G CONFERENCE

10.0F Consortium Network(Co-Net): System and Architecture Towards 6G

未来移动通信论坛
FUTURE MOBILE COMMUNICATION FORUM

Catalogue

Abstract

With the construction and application of 5G networks, mobile communication networks have achieved significant results in many areas such as people's livelihoods and vertical industries, meanwhile demonstrating tremendous commercial and social value. 6G will further expand and integrate with much more fields such as information consumption, real economy, and so on. The new 6G network will become a comprehensive platform for the integration of ODICT, covering air-space-ground integration and services such as communication, sensing, computing, intelligence, and trustworthiness.

Driven by the pluralistic new-value in the future, the original business operation models of various industries will continue to undergo evolution and experimental innovation to adapt to changing ecological demands. This will promote the reorganization and iterative updating of the ecological system, ultimately forming an integrated and innovative ecological system. Traditional "centralized" and "universal" network design and operation paradigms will be difficult to meet the various needs of the future ecological system. This white paper proposes the "consortium network" ecosystem, which is a system architecture that enables the circulation of resources and services through the collaboration of multiple networks. It is composed of multiple owner networks, and its participants can be individuals, families, government, enterprises, operators, etc. Through the consortium network, multiple consensus trustworthiness and rights protection can be achieved, enabling flexible sharing and trading of resources and services between the owner networks.

This white paper is mainly composed of six parts, including the new network ecology concept, typical scenarios and applications, design principles, architecture, related key technologies, as well as summary and prospects. The first chapter started from the value factors and fusion trends of the 6G ecosystem and proposes the ecological concept of the consortium network. The second chapter elaborated on the

typical applications, benefits, and potential new business models of the consortium network from three typical application scenarios: personal and home networks, government-enterprise and industry networks, and air-space-ground integrated networks. The third chapter described the typical characteristics of the new network model of the consortium network based on the new ecological concept above-mentioned. The fourth chapter proposed a “three-horizontal and two-vertical” consortium network architecture. The fifth chapter elaborated on the key technologies of the consortium network architecture. Finally, the sixth chapter concluded the paper and looks forward to future developments.

Explanation of Key Words in the Paper

Word	Definition
Network Owner/ Owner	The owners of various types of networks or terminal devices that participate in various activities within the consortium network (such as operators as one type of owner, or industries, enterprises, households, and individuals as different types of owners) typically use their corresponding identity within the consortium as their identifier within the network. These owners can generally be mapped to legal persons, such as operators, enterprises, or individuals, or consortium with legal person status (e.g., a vehicle networking consortium).
Owner Network/ Network	The networks that are owned by operators, industries, enterprises, households, or individuals(whether they be operator networks, industry networks, enterprise networks, home networks, or personal networks).
Consortium Network/ Co-Net	A cross-industry ecological network system formed by the interconnection of multiple (distributed and autonomous) owner networks through specific protocols (such as service registration and discovery), based on multi-party consensus. This system enables flexible sharing and trading of resources and services among various types of network owners.

1. New Network Ecosystem Concept Towards 6G

In the traditional mobile communication industry, operators have played a leading role in connecting various ecosystem partners such as equipment vendors and terminal manufacturers With the development of 5G integrated application in multiple fields such as information consumption, real economy and livelihood services, , the role of mobile communication network has gradually evolved from primarily serving mobile terminal users to serving the whole industry and even industrial ecosystem.

In the 6G era, this evolution will further accelerate. The 6G network will become a comprehensive platform for the convergence of ODICT (Operation, Data, Information and Communication Technology), with air,land,sea and space complete coverage worldwide. It will provide services such as communication, sensing, computing, intelligence, and trustworthiness, enabling a wide range of new applications and services.

1.1. 6G Ecological Value Factors

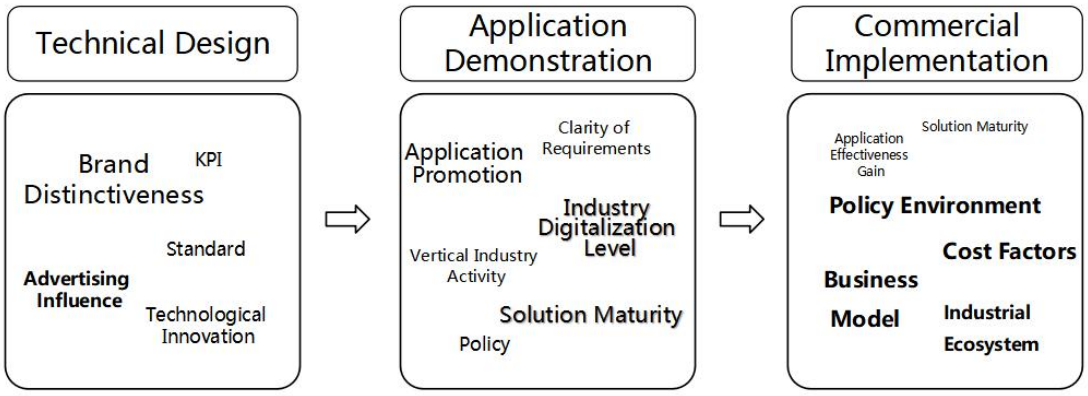

Figure 1-1: The Value Factors of Different Stage of Mobile Communication Networks

With the deepening application of ODICT in vertical industries, the determining factors for the effectiveness of communication technology applications have become more complex, evolving from performance requirement to multiple factors, including

industrial ecosystem, policies, and overall solutions. These influencing factors cover multiple levels such as the upstream and downstream industry chains , external environment, etc. As shown in Figure 1-1, the process of integrating ODICT into various industries can be divided into three stages: technical design, application demonstration, and commercial implementation. The values and development factors are different in each stage. In the technical design stage, the main values and development factors include performance indicators of the technology, standard , and technological innovation. At the same time, the influence of external promotion and brand distinctiveness are also very important. In the application demonstration stage, as the technology deepens into various industry fields, the digitization level of the industry, the maturity of the solution, and the acceptance of new technologies by application enterprises will directly affect the effectiveness of integrated applications. Once the application demonstration is fully validated and enters the stage of commercial implementation, the overall industrial ecosystem environment factors such as profit margin, cost , business models, and operation models will become more important. If a good business model cannot be established and implemented, it is difficult to maintain and develop the ecosystem. At the same time, this stage will also directly reflect the supportive role of 6G in national policies and social livelihood.

At present, 5G technology has been deeply demonstrated and explored in many industries, and some projects have entered the stage of large-scale implementation. With the deepening and expansion of industry applications, 6G will face more demands for ecologically commercial implementation, assume more responsibilities, and provide support for various industries such as information consumption, real economy, and people's livelihood services. In the future, 6G technology will face challenges in adaptability, evolution, business models, green development, and other aspects. This also means that the value and development factors of 6G networks are constantly diversifying. These factors not only reflect the key challenges of 6G, but also are the key value factors that determine the effectiveness of 6G network applications.

1.2. 6G Ecosystem Integration Trends

In the early stage of exploring the integration of ODICT applications, the technical design stage usually starts from the characteristics of each technology, then designs or searches for application scenarios, and mainly uses the Key Performance Indicator (KPI) to evaluate the effectiveness of network applications. Different technologies with similar application effects are often in a competitive relationship. With the exploration of new application scenarios, and after a period of application demonstration, the focus of integrated applications has gradually shifted to large-scale commercial implementation. In the process of potential application to commercial implementation, The importance of subjective indicators including KVIs (Key Value Indicators) such as adaptability, cost, ease of use, and KDI (Key Development Indicators) such as regulations, standards, new business models, and the restructuring of the industrial chain ecosystem, is gradually becoming prominent. The competition between various technologies is not only about technical indicators, but also a comprehensive trade-off between the overall application effect and cost-benefit. The future 6G era will shift from technology substitution and integration to ecosystem substitution and integration.

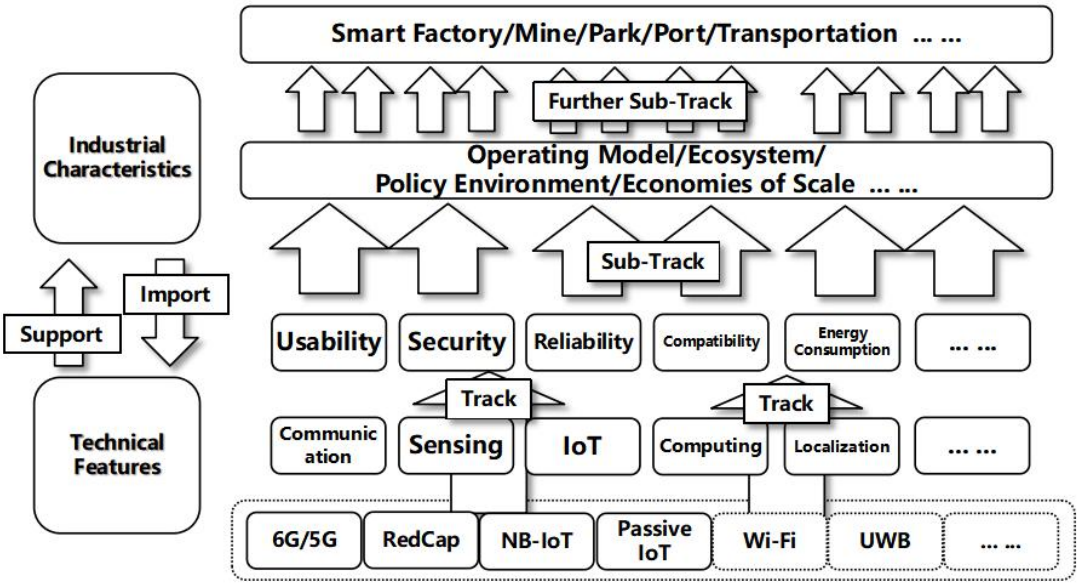

Figure 1-2: 6G Ecosystem Integration Trends

As shown in Figures 1-2, 6G/5G, RedCap, NB-IoT, and Passive IoT have different focuses during design and planning, and each plays its own role in different tracks. The final implementation of technology requires a comprehensive selection of technical characteristics (KVI indicators) and industrial characteristics (KDI indicators). The final application scenario may be divided into multiple sub tracks, and each technology (Passive IoT, RedCap, 5G, Wi-Fi, UWB) based on its technical and ecological characteristics occupies one or several tracks. Eventually, a certain balance may be reached. There is a trend of collaboration of various technologies in future applications, rather than a completely substitutive and purely competitive relationship. For example, some technologies have a competitive relationship in the positioning of the main track, but due to differences in usability, safety, and cost factors, the final application is adapted to different sub scenarios, finally forming a related industrial ecosystem.

1.3. Concept of Consortium Network Ecology

With the deepening development of 5G network and ODICT integration shift from exploration of technology integration to integration and reconstruction of industrial ecology. In order to meet the diverse application needs of industries, industrial characteristics and technical characteristics are also interdependent. Technical characteristics originate from the demand introduction of industrial characteristics, and technical characteristics also support industrial characteristics. At the same time, various industries will also work together to find the most suitable operational and business models, and through continuous exploration and iteration, ultimately form a new and benign integrated ecosystem.

The design concept of consortium networks is connecting multiple owner networks through specific protocols (such as service registration and discovery) on the basis of multi-party consensus trustworthiness, forming a cross industry ecological network system. This system allows for flexible sharing and trading of resources and services among various types of owner networks, thereby reflecting the value of each

own in the consortium network and organically integrating the ecology in which each own operates, better adapting to the diverse customized needs of various industry applications. The system can also design more flexible business models, operation models, and pricing models, making the network more suitable for the trend of ecological integration in future development, and better serving and applying the network to various industries, ultimately forming a healthy operating ecological environment.

2. Typical Scenarios and Applications of Consortium Networks

The consortium network covers various owners such as individuals, families, governments, agencies, enterprises, and operators. These owners are able to integrate their network resources into the consortium network, achieving mutual benefit. On the one hand, each owner can purchase and use the functions and services provided by other owners in the consortium network; On the other hand, the network resources can also be provided and sold to other owners for network use, and corresponding benefits can be obtained from it. The consortium network is an interconnected trading platform that enables various owners to achieve security, trustworthiness, and rights protection. It not only provides low-cost access to functions and services, but also increases monetization capabilities, which can organically integrate the network ecology of various owners.

2.1. Typical Scenarios

(1) Personal and Home Network

In personal and family scenarios, individual and family owners can add personal or home networks to the consortium network. The minimalist form of personal network can be generated by a single terminal device, such as mobile terminal hotspots, personal low altitude flying devices, intelligent connected vehicles, gateway devices, etc. Expanding operator networks from base stations to personal and home networks through various communication technologies is a cost-effective deployment solution for future networks, which can fully utilize the potential of personal and home devices to solve network coverage problems and enhance terminal communication capabilities. At the same time, individuals and family owners can rent out their network resources to other owners through the consortium network to obtain corresponding profits.

Under the consortium network system, personal and home networks can become a part of the 6G network ecosystem, playing an important role in global coverage, ubiquitous connectivity, and other aspects. It not only effectively extends high-frequency coverage, but also creates a new network sharing ecosystem for terminal light asset networking. At the same time, it has also built a new bridge for the integration of ecological applications such as personal health management, smart homes, and the Internet of Vehicles.

(2) Government, Enterprise and Industry Network

For government, enterprises, and industry owners, their affiliated enterprise networks, park networks, or industry networks can be included in the consortium network system. For example, enterprise parks can share their deployed network equipment with operators and rent their network spectrum and purchase network operation and maintenance services through consortium networks. In order to meet the privacy and security requirements of enterprise network construction, data processing and other tasks are left local, and only the necessary services are purchased from operators, reducing the cost of enterprise network operation and maintenance. At the same time, enterprises can also provide computing, storage, data and other network resources to other networks through consortium networks, reducing the cost and complexity of network deployment while maximizing the value-added of their own resources through service flow.

For operators, this approach can reduce network construction costs and be combined with industry dedicated networks to provide customized, cost-effective solutions for different types of enterprises. Under the consortium network system, innovative models of on-demand transactions have emerged between networks, such as buying to renting, with companies establishing networks and operators renting some of the company's network services. The enterprise network can also replace the operator's network to provide access functions, which can reduce network limitations, improve the cost return speed of vertical industry network services, and expand the coverage range of the operator's network. The capabilities of both parties can be expanded, achieving a double-win situation.

(3) Integrated Network of Air, Space, and Ground

The integrated network of space and ground is an important new type of network architecture in the future, which involves multiple owners such as ground operators, satellite operators, government, enterprises, and individuals. In terms of actual deployment and operation, due to the involvement of multiple stakeholders, the interests and goals of each party may differ. The consortium network system can better coordinate the interests of all parties, balance their needs, and ensure the smooth progress of network construction and operation. Satellite operator A can dynamically share satellite network resources with satellite operator B through the consortium network. Low Earth orbit satellites can be shared by ground operators C of other countries when they move to different countries. Through the consortium network, platform sharing between countries can be achieved, providing ubiquitous connections, etc. And targeted services can be provided according to needs, such as satellites only used for signal transmission to meet the data security needs of ground operators in other countries.

In the scenario of air-space-ground integrated network, it involves multiple factors such as cross domain, cross-border, and cross operator trustworthy security, rights protection, as well as cost control and performance experience of the entire system. The architecture of the consortium network is very suitable for solving complex business scenarios involving multiple parties and owners. Through a decentralized security architecture and rights protection mechanism, the consortium network flexibly shares and trades resources and services between various types of owner networks. Thus, the value of each owner in the consortium network can be reflected, more suitable for complex and diverse customized needs, and more flexible business models, operation models, and pricing models can be designed.

2.2. Typical Applications and Services

In the ecosystem of consortium networks, each owner network can provide its own resources in the form of functions and services to other networks for use and gain

profits. The potential functions and services that can be provided include:

(1) Leasing of Spectrum, Computing Power, and other Resources

In the future, various applications oriented to virtual and augmented reality, 8K video stream, holographic projection, smart home, fog computing, integrated artificial intelligence services, unmanned aerial vehicles and autonomous vehicle will sharply increase the demand for spectrum and computing power and other resources. Through the consortium network, the efficiency of spectrum utilization can be improved, and more possibilities of new resource management methods can be brought. And through the rights system, the consortium network can also establish a trustworthiness and cooperation environment across owners, thereby achieving dynamic cross operator spectrum sharing. At the same time, using encryption and anonymization technology, the consortium network can protect the privacy of spectrum sharing participants and the security of shared data, and can achieve optimal spectrum allocation on smart contracts through algorithms.

(2) Sharing of Data, Models, and other Resources

With the development and application of artificial intelligence, the demand for sharing data, models and other resources in the future is gradually increasing. Unlike leased resources such as spectrum and computing power, the rights protection system for data and big models is more complex due to the involvement of privacy, ownership, and secondary development value. Traditional purchase and lease models cannot maximize the rights and interests of data and model providers. By utilizing consortium networks, data and models can be flexibly formulated and traded. In addition, the consortium network can introduce a reasonable reward mechanism to promote resource sharing, thereby improving the utilization and benefits of various types of resources in the owner network of the consortium network.

(3) Roaming Services such as Cross Owner Access Switching

Through the consortium network, it is possible to coordinate independent owner networks, fully utilize the network resources of individuals, families, government, enterprises, and operators, achieve ubiquitous access, and provide secure and flexible authentication/authorization settings, providing users with more convenient cross

owner network roaming access, ensuring wireless service continuity. On the other hand, it can also change traditional static protocols, regulate the behavior of various owner networks within the consortium network, create a community of interests, improve the flexibility of roaming protocols, and improve cost-effectiveness, achieving safe sharing and double-win within the consortium network.

(4) Trusted Security, Rights Protection and other Services

In addition to the sharing, leasing, and trading of network resources and capabilities among various owner networks, the consortium network can also provide trusted security, rights protection, and other system platform services for each owner through its own system architecture. For example, by providing services such as identity authentication, privacy protection, asset verification, and transaction protection for owners, the consortium network can serve as a more comprehensive, secure, and trustworthy platform, providing broader support and protection for various owners.

2.3. Concept of New Business Model

Through the design of consortium networks, there are more possibilities for future network business models, and some potential new business models can be summarized as follows:

① Change of asset ownership mode. For example, the transformation from heavy assets to light assets, and from purchasing physical products to purchasing functions and services. In the design of the consortium network, the owner can select the network functions and services provided by other owner networks according to its own needs. The consortium network becomes an integrated business platform that can provide a variety of service modes, capitalizes the capabilities of each owner network, and can select corresponding network application modes according to the needs. Possible ways are as follows:

- Basic function transaction mode: such functions as basic connection, calculation, storage service, communication control and execution, including paging, access,

mobility, etc.

- Platform service transaction mode: such as industrial application operation, network performance management, intention engine, use case analysis, intelligent decision-making, data search, data analysis, etc.
- System transaction level service mode: such as digital assets, blockchain services, etc.

② Change of network construction mode. In the traditional network, it is often limited by the cost of network construction, and can not fully meet the personalized needs of network construction. By using the consortium network, the network deployment, construction, operation and maintenance methods can be very flexible, which can achieve accurate positioning of needs, and provide customized services quickly, accurately and at low cost.

③ Change of pricing and billing mode. By using the trusted security, rights protection and other systems of the consortium network, and combining the extreme customization and service type selection of the above two points, it is expected to achieve more targeted pricing and billing methods between networks, including rent, purchase, on-demand, quantity based, on time and other modes, so that the demand sides can obtain corresponding services at a lower cost.

In the consortium network system, more new business models that adapt to diversified needs in various fields and industry applications become possible. Such models can create business operation models and ecosystems that adapt to the characteristics of future diversified network needs, which is one of the important values of the consortium network. Under the adaptive operation and business model, the network can better serve various industries, thus forming a benign operating ecological environment.

3. Consortium Network Design Concept

According to the ecological concept of the consortium network, the network ecology of multiple owners can be organically combined. Through the collaboration between networks, network resources and network functions can flow among networks in the form of services, expand the service scope of each network owner, and allow flexible sharing and trading of resources and services between various types of owner networks, so as to reflect the value of each owner in the consortium network. The consortium network can adopt flexible business mode, operation mode and pricing mode in different scenarios for various customized demands of industrial applications, but they all have common characteristics. The basic characteristics of the consortium network are as follows:

3.1. Network Autonomy

Network autonomy is the basic requirement of consortium network. The most basic unit in the consortium network is the owner network, with convenient functional organization and its own unique application scenarios and needs. Each member of the consortium has independent decision-making power and control power, and can independently manage their own resources and traffics without being affected by other members. Each member can manage and configure its own network according to its own needs and policies. Its infrastructure rules, connection protocols, service-oriented functions, and openness can be customized according to scenario requirements, so as to better adapt to different business scenarios and needs. For example, in the ToB (To Business) scenario, vertical industries can independently build and manage networks according to their specific requirements to achieve full customization. This autonomy helps ensure the flexibility and scalability of the consortium network, enabling it to adapt to changing needs and environments.

3.2. Flexibility of Service Relationship

Flexibility of service relationship is one of the important characteristics of consortium network. On the one hand, the owner network capabilities in the consortium network vary considerably, and the specialized and extremely simplified network needs services provided by other networks. On the other hand, the communication-sensing, artificial intelligence, computing power and other functions of the network cannot be optimized simply without the help of edge networks and terminals. Therefore, in the future, the service relationship between the various owners in the consortium network will change. Not only the operator network can serve as a service provider, but also various owners in the network can provide services and obtain benefits according to their capabilities. This will build a new network ecology, which means that the network is not only a kind of consumption, but also an infrastructure that can widely generate productivity. All owners using other owner networks can achieve production and consumption through the network. From the perspective of infrastructure construction, various owners other than operators can build communication facilities in the authorized frequency band with permission. End users can access the network through such communication facilities. Operators rent or authorize other owners to operate communication facilities, and the owners can obtain income through rent and service sharing. In terms of services, various owners can provide operators with services such as computing task offloading, AI (Artificial Intelligence) learning assistance, and surrounding awareness, and operators pay for services. From the perspective of data, various owners can gain income by selling or leasing their digital assets. On the one hand, the owner can obtain benefits by assisting the operator. On the other hand, in addition to the interaction between owners and operators, owners can also interact with each other to gain benefits, such as providing relay for remote users in other owner networks, providing data cache for other owners to reduce transmission delay, etc.

3.3. Distributed Collaboration and Sharing

As one of the core characteristics of the consortium network, distributed collaboration and sharing emphasize the collaboration between networks. There are different kinds of networks in the consortium network, including the large network of operators, the government, enterprise and industry network. Through cross-network, cross-region and cross-business cooperation, the consortium network is formed to be a closer whole and achieve the common goal. By sharing network resources and functions, the owner network can acquire capabilities beyond its own, avoid repeated construction of the network, and improve the efficiency of resource utilization. This also helps to reduce the threshold for deploying networks, making it possible for simplified networks, which is of great significance to the ToB industry. For example, small and medium-sized manufacturing enterprises do not need to build a complete network by themselves. They just need to deploy access network nodes and service routing gateways, and realize core networks, auxiliary computing power, artificial intelligence and other resources through the sharing of other networks, effectively reducing the cost of trial and error for enterprises. The distributed collaborative architecture has good scalability and can flexibly support application scenarios of various scales and complexities. Through the sharing of network resources and functions, it can realize the rapid deployment of the network and flexible expansion of various applications and services, meet the growing network needs, reduce the cost and time requirements of network updates, accelerate network iterations, and improve the performance and quality of service of the entire network. Through distributed collaboration, the network can better support various new businesses and applications, such as virtual reality/augmented reality, automatic driving, etc. Both large-scale IoT and small-scale smart home can be effectively supported under the distributed collaborative architecture. This helps to improve the user experience and meet the diverse needs of users. Distributed collaboration can reduce the operation and maintenance cost of the network, reduce the dependence on the central node, and improve the adaptability and maintainability of the network. Through distributed

deployment and collaborative work, the system can achieve load balancing and fault redundancy between different nodes, thus improving the reliability and stability of the entire system. Distributed collaboration combines technologies such as decentralization and cryptography to provide better security and privacy protection and ensure the security and integrity of user data.

3.4. Multi-party Trustworthiness and Security Privacy

All network owners in the consortium network are equal, and there is no upper central node, so the consortium network relies on multi-party negotiation to ensure the trustworthiness of the entire network. Multi-trustworthiness provides trustworthiness through multi-owner negotiation and consensus, and ensures the trustworthiness of interaction according to the algorithm of blockchain like consensus mechanism. Multi-party trustworthiness also includes a smart contract mechanism that runs automatically, achieving that multi-party confirmation is a fact, which avoids the risk of unilateral default. The multi-party trustworthiness guarantees the trustworthiness of the network in different scenarios and needs, and realizes trustworthiness between any node in the whole network. Multi-party trustworthiness also includes distributed digital identity, which is an interactive credential. Distributed digital identity can achieve autonomous control of identity, generate real-time digital identity with different contents according to needs, and protect other information of identity from exposure. The consortium network realizes active security immunity by Mimic Defense, distribution and AI, forming the native security of the network. In addition, for the interactive content, the identity of the transmission receiver and the transmission content are encrypted through symmetric encryption and asymmetric encryption technology in the information transmission dimension, and privacy computing is used in the information processing dimension to ensure that data processing does not disclose information.

3.5. Intelligently Automatic Operation

Intelligently automatic operation in the consortium network is not only used to improve network operation and maintenance efficiency and enhance network communication performance in traditional networks, but also used to ensure multiple interactions. The consortium network realizes the trusted interaction process between various owners through multi-party trusted technology. Due to the lack of central nodes or central institutions, the enforcement of third-party guarantees cannot be achieved. Therefore, the consortium network realizes the interaction and automatic execution of contracts through intelligence. If a contract is formed through consensus, funds will be transferred after the service is completed. The use of traditional methods may cause problems such as fund delay and arrears. The consortium network uses an intelligent way to ensure its operation. It adds an intelligent automatic execution function to the contract, and automatically transfers funds after the service ends. The service provider cannot prevent this behavior from happening through coercive means. Not only in the field of contracts, but also in other interaction modes, intelligence can ensure the reliable interaction.

4. Consortium Network System and Architecture

4.1. Overview of System and Architecture

The architecture of an consortium network can be summarized as "three horizontal and two vertical", consisting of three layers including the owner network layer, interconnection layer, and network application layer, as well as consortium rights management and consortium trustworthiness guarantee that run through the three layers. The owner network layer is the foundation of the consortium network, which includes various owner networks in the consortium network, each with its own identity, resources, services, etc. On top of it is the interconnection layer that connects various owner networks, providing the ability to register, discover, and call services, and achieving communication and collaboration between networks. At the top is the network application layer of the consortium, which provides the ability to call underlying services for various applications, and can achieve but not limited to ubiquitous access, resource sharing, data circulation and other service capabilities. Consortium right management provides strategic planning and right management functions, providing automatic contract execution, transaction strategy formulation, and other capabilities for each layer. Consortium trustworthiness guarantee provides trustworthiness and security guarantees for the entire consortium network, maintaining multiple capabilities such as multi-party consensus and privacy protection.

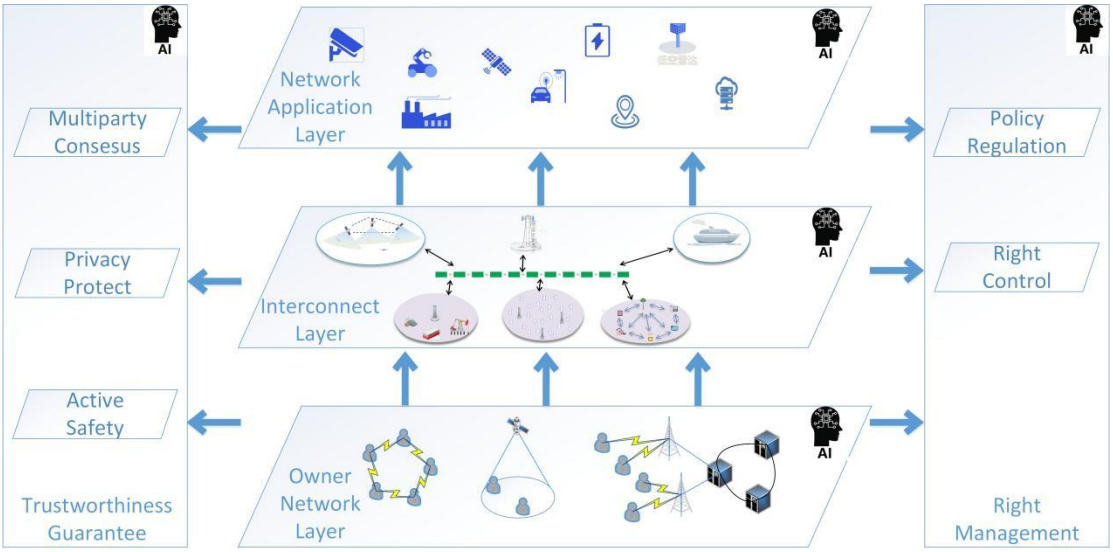

Figure 4-1: Consortium network system and architecture.

4.2. Owner Network Layer

The owner network layer is the foundation of the consortium network, composed of various independent owner networks. The owner network can be operator's networks, government, enterprise and industry networks, as well as the personal and family networks. The owner network first needs to achieve self operation without relying on external factors. It is an autonomous owner, and all decisions and management are made by the network owner. The owner can dominate the elements in the network, which is the prerequisite for forming an consortium network. The owner network can include sub-layers of networks, as well as users such as terminals. These individuals within the network interact with other external owner networks and individuals within the owner network through the owner network.

The owner network also includes three basic elements: network identity, network resources, and network data. Network identity is one of the foundations of inter-connectivity between networks. When interacting with other networks, network identity is required as a credential for authentication and an identifier for content distribution. The consortium network is a distributed network structure without a centralized management organization, so the network identity of the consortium network needs to use distributed identity mechanisms, such as DID (Decentralized

Identity). Network resources are an important component of inter network sharing and services. Resources can be wireless spectrum resources, network infrastructure such as communication, computing power, perception, or digital resources. Network data and models, together as the main elements of artificial intelligence and big data analysis, cannot adopt the same sharing policy as traditional resources, such as the management and operation data of the network itself and individual privacy data in the network。Network data and models require a specialized processing method.

4.3. Interconnection Layer

(1) Architecture Overview

The interconnection layer is the key to achieving inter-connectivity between networks, and it is viewed horizontally as a bus based network architecture. The various networks in the consortium network have equal status with others, and traditional centralized control cannot be deployed here. Therefore, the interaction between networks is achieved through a bus based interconnection architecture. Autonomous networks interact with other owner networks through interfaces on the bus, which avoids the exponential complexity of connection management that comes with increasing network numbers. And the bus architecture supports flexible network joining and exiting, without causing too much impact on other networks in the consortium network. In a bus architecture, the interaction between networks is carried out in the form of services, which have different implementation forms. The two mainstream implementation methods currently available are distributed network function management and decentralized blockchain. Distributed network function management uses Distributed Networks Management Function (DNMF) units as interactive interfaces to complete service management by forming a registry. Decentralized blockchain style uploads information to blockchain like nodes and completes higher-level service transactions through multi-party consensus mechanisms.

(2) Distributed Network Function Management

The consortium network supports high-level open and diversified networks and multi-modal network architectures. However, the discovery and management of network topology is a major challenge that needs to be addressed. Based on key technologies such as computing power, data, AI, and security, the existing NRF (Network Storage Function) and SCP (Service Capability Exposure Function) have been expanded to form a new network functional unit, DNMF.

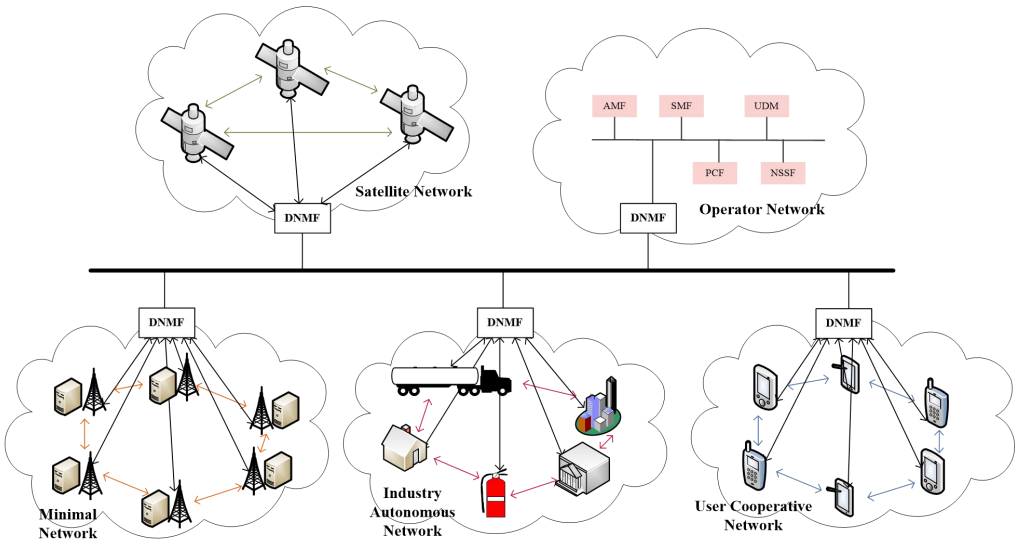

Figure 4-2: Figure 4-2 DNMF consortium network architecture

The DNMF within the consortium network not only maintains the basic information of the network control plane units, but also maintains the information,such as network function information, resource information, service information, etc, which is generated on demand based on traffic characteristics in non-operator networks. By maintaining multiple types of information, diversified network platforms can adapt to the various scenario requirements of 6G.

At the same time, DNMF provides external interfaces for various networks and undertakes the management, authentication, networking and other tasks of each network. This is conducive to achieving elastic self-organization of network topology, while implementing trusted and secure network discovery and communication mechanisms, improving the security and reliability of the entire network. DNMF is used to achieve information maintenance and updating, automatic registration,

deregistration, and preservation in network granularity. The information maintained by this network function includes the service information of owner network itself, the service information connected to other networks, and the topological connection relationships between networks. The service information includes owner identification, owner network type, DNMF address information, owner network functional attributes, owner network location information, owner network service area information, data network information, slice information, computing power resources, etc. Each network can carry out collaborative control, billing reward monitoring, main digital asset application management and so on through DNMF.

(3) Blockchain-like Decentralization

The blockchain-like decentralized architecture uses blockchain-like technology as the bus for network interaction. The blockchain modules of each network are interfaces on the bus, which can be divided into blockchain transaction consensus function modules, blockchain ledger recording function modules, and custom function modules.

When the network owner can provide services to the outside world, the blockchain module can publish service list information, digitally sign it, and then form transaction information to broadcast. If other network owners verify that the signature and information correspond, the transaction information can be written into the block. When network owners need services, they can also use the same process as publishing service information to actively publish recruitment or reward information. When the services of the network owner change, the same process can be used to publish service updates and write them into blocks. The network owner regularly receives and stores this information.

4.4. Network Application Layer

The network application layer is the highest layer in the consortium network system, and on the basis of the lower two layers, the network application layer is directly connected to the actual application. On the one hand, this layer can provide

common network basic application services, such as ubiquitous access, resource sharing, data circulation, etc. On the other hand, this layer can provide a lower level mapping management interface for other applications undertaken on it. In this regard, the network application layer has functions of calling, organizing, and aggregating, which can arrange various resources and basic functions at the lower level, map applications to relevant management and control units, provide precise on-demand support for applications, and achieve cross owner network level service guarantee capabilities.

4.5. Consortium Right Management

Consortium right management is an important support for achieving new organizational models and ecosystems in consortium networks. Consortium right management includes strategic rules and right control. The strategic rules are mainly reflected in the incentive mechanism, which plays the role of resource exchange rules. It stipulates how the network negotiates the exchange of different resources, including the quantity and value in exchange, allowing for the personalized exchange rules between networks. The representative of right control is smart contract, which is a technical upgrade version of the contract. The contract is recorded through code and is enforced when the conditions or deadlines are met. In practice, it is also necessary to cooperate with multi-party trustworthiness technology to ensure that the results of mandatory execution become a majority recognized fact. Therefore, consortium right management guides and coordinates the establishment of "contracts" between networks, and through technical design, ensures the mandatory execution of "contracts", eliminates the phenomenon of breach of contract, and effectively supports the development of various upper level applications.

4.6. Consortium Trustworthiness Guarantee

Consortium trustworthiness guarantee provides trustworthy interaction between various network owners in the entire consortium network. Due to the equal

relationship between network owners and the lack of coordination and management by upper level institutions, achieving equal exchange of resources must be achieved through negotiation mechanisms between networks. The consortium trustworthiness guarantee provides capabilities such as multi-party consensus, proactive security, and privacy protection. Multi-party consensus is the foundation for implementing incentive mechanisms, where through a certain mechanism of multi-party negotiation, consensus on resource exchange is formed. It regulates the methods used by multiple parties in the negotiation process to reach the final consensus, which can be predetermined default rules or self defined methods by multiple parties. The active security capability is formed through the distributed characteristics of the consortium network, coordinating various owner networks to form complementary active security capabilities, and achieving preventive measures. The privacy protection capability protects the privacy content of each owner during the interaction process, allowing the interaction to be supported by trustworthy owners outside of the participating parties without disclosing privacy content to the outside world.

5. Related Key Technologies

5.1. Autonomous Digital Identity

The advent of consortium networks marks a transition of communication networks from closed, unitary systems towards open, distributed, and interconnected frameworks that encompass a wide array of actors and stakeholders, such as spectrum traders, cable and satellite service providers, IoT and Over-The-Top (OTT) service providers, which play pivotal roles in network connectivity and related services[1]. Within the context of the consortium network, the role of Mobile Network Operators (MNOs) changed from conventional single network operators to the connectivity facilitators, orchestrating the interactions among a diverse set of participants. This signifies that network connectivity is transitioning into a service that spans multiple domains, dependent on the allocation of resources among various trustworthiness domains within the consortium network. As an increasing number of participants engage in the consortium networks where operations are disaggregated, the need for interfaces capable of bridging these domains grows. As a result, trustworthiness is a key design principle, necessitating to be established among all parties and their networks through unified access management.

Consortium network is running on effective coordination among participants, including cloud services, edge computing, and hardware suppliers, to cultivate an ecosystem of diverse services from stakeholders. Thus, the coordination must be economically viable and provide seamlessly connectivity. As a result, participants in the consortium network requires an interface guarantee secure authentication and authorization, fulfilling the demands of identity and key management within a Public Key Infrastructure (PKI). Therefore, consortium networks target at facilitating collaboration between various emerging and traditional participants, while maintaining security and trustworthiness within an open, distributed environment. Such a network architecture catering to the demands of future communications in

flexibility, scalability, and efficiency. Within this framework, 6G encounter a variety of challenges regarding authentication and authorization processes. For instance, 5G mobile users primarily utilize symmetric encryption for authentication. However, during roaming, operators may employ secure transport layer protocols based on asymmetric encryption and pre-shared public keys for inter-operator communication. To implement asymmetric encryption authentication within consortium networks, it is necessary to establish and maintain a complex PKI, while also ensuring secure interconnectivity among different operators.

Moreover, the lack of a globally trusted Certificate Authority (CA), coupled with geopolitical differences and the need to prevent single points of failure or attack, makes establishing a unified, centralized PKI-based identity management impractical. In 5G, GSMA recommends that each MNO operates at least one root CA to mitigate single points of failure or attack[2], but this does not solve the issue of creating a universally trusted Certificate Authority. Furthermore, the implementation of personal data protection laws like GDPR in Europe heightens user concerns over data handling. In consortium networks, MNOs find it difficult to comply with privacy and transparency regulations due to the centralized handling of personal data by themselves and their partners. Thus, in 6G consortium networks, a new, unified identity management system is essential to overcome system heterogeneity, the lack of a universally trusted CA, and heightened personal data protection requirements. The digital identity management system in 6G must meet the universal requirements of various stakeholders, including but not limited to users, IoT devices, MNOs, virtual mobile networks, cloud or IoT operators, manufacturers, and even network functions (NFs).

While centralized PKI is viable in secure and trusted settings, it faces challenges with interoperability, compliance with data protection regulations, and geopolitical constraints. Thus, consortium networks must explore alternatives, like the Decentralized Identifiers (DID) proposed by W3C[3], providing a unified, secure, and tamper-proof identity management solution across domains, eliminating the reliance on centralized authorities. owners within consortium networks, including both

space-based and terrestrial systems, can leverage smart contracts and blockchain-inspired technologies to document and safeguard service entitlements. This approach facilitates expanded services and cooperation, better preparing them to address the evolving demands and challenges of future communications. The design of self-sovereign digital identities should adhere to the following principles:

①Privacy Protection: Designed to safeguard the real identity and personal data of the identity subject, utilizing technologies like smart contracts and blockchain for secure, transparent handling.

②Interoperability: Ensure universal access and recognition across consortium network owners with a unique, machine-readable, standardized format, crucial for multi-stakeholder collaboration.

③Verifiability: Cryptographically verifiable, allowing subjects to prove their identity ownership and others to validate shared personal data, enhancing transaction and interaction security.

④Scalability: Capable of adapting to diverse applications, evolving technologies, and emerging needs, offering versatile verification methods suitable for owners ranging from individuals to corporations.

⑤Independence: Operate independently of any corporations, organizations, or governments, including identity providers and CAs, ensuring a decentralized, resilient, and secure system.

Self-sovereign digital identity introduces a novel method for identity management, enabling identities to be managed in a unified and decentralized manner without reliance on centralized identity providers or CAs. Utilizing distributed ledger, self-sovereign digital identities provide a decentralized manner for cross-domain access management within a unified network. Distributed ledgers enable the management of access records for non-privacy-sensitive data among all participants by storing permissions in a format of verifiable credential. This approach shifts from centralized to decentralization storage, with authorization data dispersed among the owners like customer devices, which reduces the risk of single points of failure or attacks upon CAs and enables MNOs to better adhere to privacy principles.

5.2. Distributed Service Management

Service management is an important mechanism in the service-baseed architecture. Compared to previous generations of traditional network architectures, 5G network functions use service-based interactions between each other, with each network function providing one or more services for other network functions. When two network functions communicate, they will play different roles. The NF sending the request plays the role of service consumer, and the NF accepting the request plays the role of service provider. Service management is the mechanism used to determine how service consumers can find service providers that provide the requested services. This mechanism relies on the centralized NF in the network, namely NRF. Other NFs in the same network register their services to the NRF, which then manages the services they provide. The service invocation between different networks further depends on the interaction between the NRFs of each network.

For 6G consortium network, the distribution trend of network architecture will be more significant. The entire consortium network is composed of numerous independent owner networks belonging to different owners. owners can not only be operators, but also government, enterprise, industry customers, or individual and household users.The form of owner networks also far exceeds the scope of public land mobile networks constructed by operators.

Considering the flexibility of service relationships in alliance network, the signaling involved in service management need to carry more information, and the frequency of occurrence will also increase. The traditional NRF-based management mechanism need to be further enhanced to meet requirements of distributed service management, while introducing function like SCP to achieve service routing and forwarding between networks. In addition, diverse network ecosystem participants mean that service management mechanisms need to build a trustworthy and fair operating environment, and provide distributed service management capabilities to encourage cooperation among all parties, ultimately achieving efficient flow of resources and data throughout the entire alliance network. Finally, the current service

management of 5G networks mainly focus on the NF level, while the distributed service management of alliance networks need to further consider network-level discovery and negotiation issues..

As a distributed accounting system, blockchain is an organic combination of a series of existing mature technologies, including distributed consensus, peer-to-peer communication technology, etc. It effectively records the ledger and supports different business logic. From an external perspective, blockchain systems have the characteristics of multi-party writing, joint maintenance, public ledger, decentralization, and immutability, making it naturally suitable for the various demands of distributed service management in consortium networks.

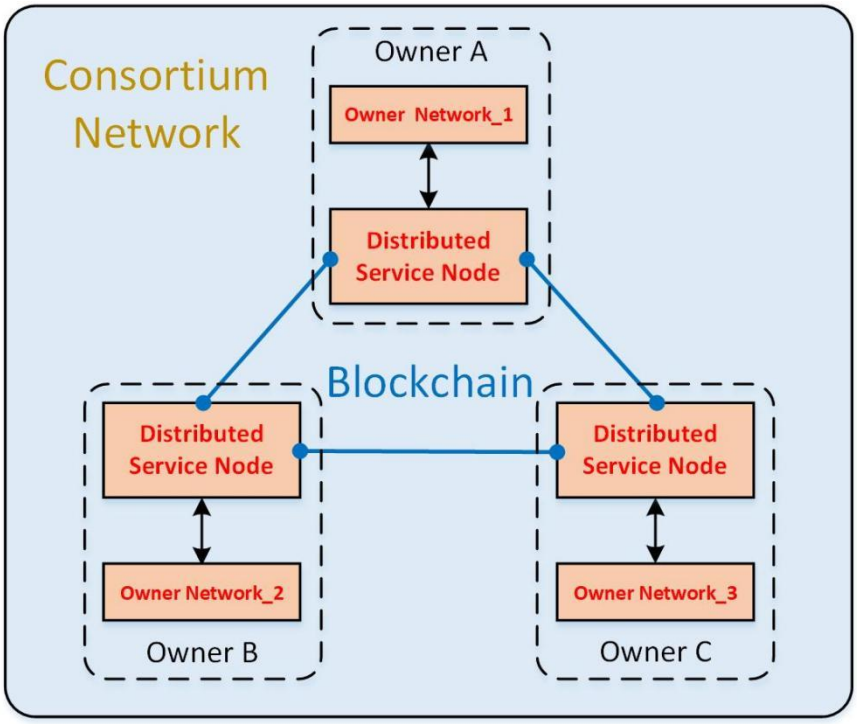

Figure 5-1: Blockchain based distributed service management solution

The overall description of the blockchain based distributed service management scheme is shown in Figure 5-1. In the consortium network, there are several independent owner networks, each of which deploys service nodes representing its own owner. These service nodes, as blockchain nodes, together form a blockchain network as the distributed service management base of the consortium network. Service nodes provide service registration, update, deletion, invocation, and routing negotiation for the owner network, and record service information and invocation

records on the blockchain. By utilizing features such as smart contracts and chain data structures, the solution achieves the recording and protection of service rights, providing a method to protect the interaction between owners within the consortium network that share common goals but do not fully trustworthiness each other.

Specifically, each owner network joining the consortium network initiates registration/update/deletion requests for network capabilities or NF services to distributed service nodes belonging to the same owner. The distributed service node that receives the request will write the request content into the transaction, and the blockchain network will reach a consensus on the transaction. Autonomous networks can query blockchain through distributed service nodes at any time to obtain the necessary information. When specific content is needed, the distributed service nodes negotiate routing, record call records on the blockchain, and ultimately complete the call.

5.3. Right Management

Right includes rights and interests, generally referring to the roles, status, rights, and benefits assigned to owners. The protection of right not only promotes fair competition among various network owners, enhances cooperation and trustworthiness, but also benefits network stability and sustainable development, which is crucial for the success of consortium networks. The protection of right needs to be supported by right management, which can be divided into three functions: right strategy, right control, and right execution.

Figure 5-2: Right in consortium network

Right strategy is the management of policy rules in the network. In consortium

networks, there are various types of network owners. For example, in the internet of vehicles, there are various network owners such as vehicle manufacturers, telecommunications operators, software and platform providers, government agencies, insurance companies, maintenance and service providers, and data analysis companies. These owners collaborate with each other in the car networking ecosystem, jointly promoting the development and application of car networking technology to improve traffic safety, efficiency, and convenience. By clarifying right of all parties in the network through strategic rules, it is possible to balance and coordinate the needs of various owners, which is conducive to achieving multi-party governance and double-win outcomes in the internet of vehicles. It can be seen that right strategy formulation is the core of right management. Specifically, right strategy management includes the formulation of various strategic rules such as owner control, right division, and right trading. The control strategy rules for right owners include judgment of owner qualifications, legality, provisions of laws and regulations on owners, provisions of contract agreements on owners, and confirmation of owner identity. The right owner control strategy ensures right of legitimate owners and prevents illegal or non compliant owners from obtaining right. The right content strategy rules clarify the ownership rights, network information rights, service usage rights, and other rights of each owner in the consortium network, as well as the incentives/rewards that each owner should receive for their contributions to the network. The right trading strategy rules stipulate various rules that both parties must comply with during the transaction process, such as whether there is third-party proof, how to control the transaction cycle, whether the transaction is revocable, whether to agree to scoring, specific scoring strategies, how telecom blockchain selects ledger, whether privacy protection is required, and the degree of privacy protection.

Right control is the management and control of the process of right interaction. There are many processes of rights interaction in the network, such as rights configuration confirmation, rights registration discovery, rights request response, etc., which require interaction between both and even multiple parties of the network owner. The process of confirming right allocation refers to the network determining

the right information of participating owners (such as ownership, management, pricing, sharing ratio, etc.) based on right strategy rules, and sending the right information to the corresponding network owner that owns the right, so that the network owner can not only understand its own rights in the network, but also choose to accept or reject the rights configured by the network. The process of discovering rights registration refers to each network owner being able to register the rights information corresponding to the resources and services they provide to a centralized rights information database or use blockchain, so that users of resources and services can conduct fair transactions on the premise of seeing and recognizing these rights information. The process of rights request response refers to the network owner actively initiating requests for its own rights based on its own capabilities, and the management party (such as notary public, trading platform party) or user in the consortium network responds to the rights request.

Right execution is the management of the actual execution process of right strategies and right controls. Right execution involves a series of operations and activities related to right to ensure the effective implementation and maintenance of right management. Specifically, the operations carried out by rights include: determining and setting the rights of network owners, querying rights of network owners, modifying or updating rights, terminating or revoking rights of network owners, and restoring terminated or damaged rights.

In right management, right strategy provides guidance for right control and right execution. Right control ensures the effective implementation of right strategy, while right execution is the specific means to achieve right strategy. Through the collaborative work of these three functions, comprehensive protection of right of network owners can be achieved.

5.4. Multi-Party Consensus Based Trustworthiness

In distributed systems, the lack of a commonly trusted centralized authority leads to the unreliability of resource and service exchanges between nodes. Consequently,

there is a pressing need for trustworthiness establishment. One approach involves establishing a trustworthiness evaluation system based on past behavior of nodes, where one could determine the confidence level of nodes through credit scoring. However, its efficacy is contingent on the history of interactions, limiting its reliability for new or infrequent interactions. To overcome this limitation, the concept of multi-party consensus has emerged, fundamentally establishing trustworthiness through the collective participation and negotiation of multiple parties. A typical realization is blockchain-based consensus mechanism, which utilize decentralized ledgers and smart contracts to enable autonomous trustworthiness establishment and management, eliminating the need for external validation.

Blockchain addresses data security and sharing issues in traditional communication networks by enhancing network resilience and adaptability in environments where trustworthiness is not assumed. Early in consortium network development, integrated blockchain plays a crucial role, allowing for tight interaction between the blockchain and communication networks, encompassing both offline and online interaction. For instance, in blockchain-based identity verification, information owners or authorized parties store credentials or hash values on the blockchain. Through a communication request, a network owner verifies the credentials of requester against the blockchain. If authentication successes, the connection request will be accepted, enabling a flexible and secure verification mechanism within consortium networks.

As consortium networks evolve, blockchain will become increasingly integrated and embedded to communication networks, developing into an essential component. In this integration, blockchain algorithms, communication protocols, and enabling functions will be fully incorporated into the functionalities and protocols of communication networks. In such an intertwined form, blockchain operations, including writing and searching, will occur in real-time and online as part of the communication process. Implementing blockchain technology in communication networks for real-time applications presents several challenges, and three core objectives must be prioritized:

1. Blockchain Theoretical Basis for Consortium Networks: Consortium Networks require a real-time and scalable blockchain system as a reliable foundation. Developing theories specifically designed for consortium networks, while considering the distinct features of various network types, is crucial to guarantee the successful application of blockchain in a range of diverse and evolving environments.

2. Adaptive Blockchain Architecture for Consortium Networks: The architecture needs native design to meet the unique demands of consortium networks, including deterministic low latency and high throughput, and privacy considerations. It is crucial to develop an architecture that efficiently processes data and signaling, ensuring immutable recording.

3. Blockchain Platform Tailored to Consortium Networks: Building a cloud-edge integrated blockchain platform tailored for communication networks is vital in facilitate the exchange of services and resources among network owners, accommodating various forms of networks.

5.5. AI Empowered Network Intelligence

The interaction between the owner networks in consortium networks is frequent, and relying solely on fixed strategies and manual control is rough and slow. At the same time, it cannot meet the trustworthiness of the interaction. Therefore, intelligently automatic operation has been widely applied in consortium networking. By utilizing advanced algorithms and model libraries, including machine learning, deep learning, and reinforcement learning algorithms, and through large-scale language model training and distributed generation of multiple networks, the entire network can achieve a higher level of autonomy. The network can achieve functions such as automated decision-making, resource management, and traffic scheduling. This will help improve the operation efficiency and response speed of the network, and reduce operation costs. For example, nodes can collaboratively adjust routing and traffic allocation based on traffic load conditions to improve network performance. At the same time, intelligently automatic operation will also support personalized service

needs, providing users with a higher quality and efficient network experience. As the environment and traffic requirements change, the network can automatically adjust its operating parameters and strategies to adapt to the changing environment and requirements. This helps to improve the flexibility and scalability of the network. Intelligently automatic operation is also reflected in the rapid response and handling of abnormal events. By monitoring and analyzing network status data in real-time, the network can detect abnormal events in a timely manner and handle them quickly. This helps to reduce the risk of failures and improve the reliability of the network. Meanwhile, intelligent automatic operation also helps improve the adaptability of the network.

5.6. Other Technologies

(1) Rapid Establishment of Network Services

With the assistance of multi-party consensus and distributed service management, multiple network owners within an alliance network can establish network service with clients, part of whom are even not affiliated with the subjects. Simultaneously, with the exponential growth in access demands, the quality of service (QoS), multi-party management, and security are confronted with significant challenges. The technology for fast establishment of network service will provide an efficient and secure provision of network services under the premise of ensuring QoS, thus offering a solution to the dilemma of cross-domain access in the alliance network.

In conventional schemes, clients are required to sign contracts with network owners in advance if they want to be offered network service. Only after building trustworthiness between clients and subjects can the network owners provide the required service to the clients. However, through the technology of fast establishment of network service, the subjects can immediately provide network service to clients once the clients send requests. By splitting service and signing smart contracts multiple times, the technology can skip the complex process of establishing trustworthiness and thereby manage to rapidly establish network service.

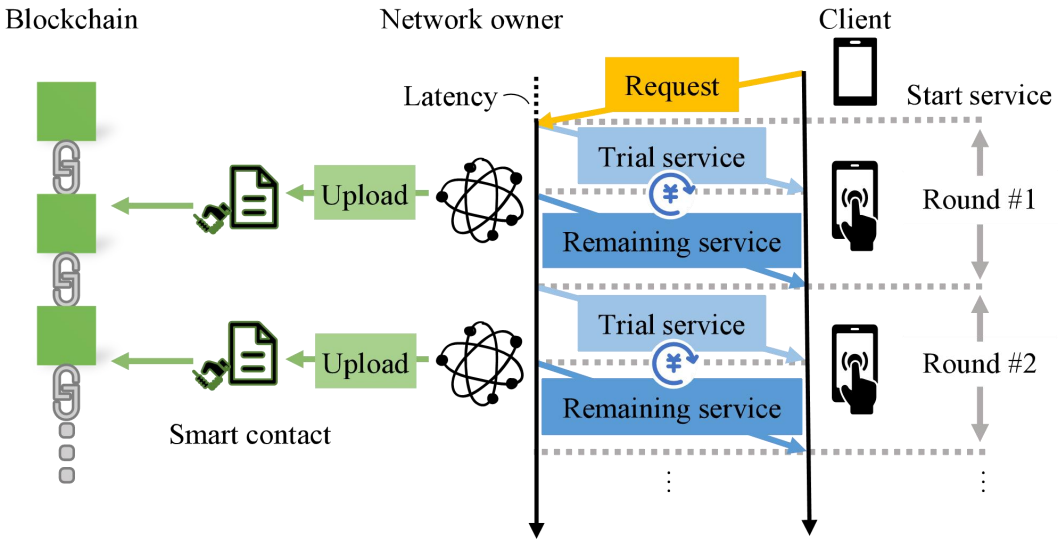

Figure 5-3: Scheme for establishment of network service

Fig. 5-3(b) illustrates the working principle of this technology, whose workflow can be described as follows.

① In the beginning, the client sends a service request to the network owner within the alliance network.

② Upon receiving the request, the network owner immediately provides service to the client.

③ The whole service process is divided into multiple rounds. Each round begins with a trial service for a given duration provided by the network owner.

④ Before the end of each trial service, the client commits to paying the fees to the network owner by signing a smart contract. The fees include the cost for the trial service the client already received and the cost for the remaining duration in the current round, thus compensating for the risk the network owner takes in offering pro bono services.

⑤ If the client honestly signs the smart contract and commits to paying as demanded, the network owner immediately provides the rest of the service and also uploads the smart contract to the blockchain network before the end of this round. Once the block containing the smart contract is successfully added to the blockchain, the fees are automatically transferred from the client to the network owner.

⑥ If the client refuses to pay in respect of the smart contract, the network owner ceases to provide the rest of the service and terminates their cooperation.

⑦ If both sides act honestly, they can complete the round and then start a new round by repeating the steps above until the successful completion of the whole service.

⑧ The client can terminate the service by refusing to pay in a specific round, and the network owner can stop providing services as well to halt the cooperation.

This cross-domain access framework for fast establishment of network service has the following advantages:

① If clients are unsatisfied with the network service provided by the subjects in the alliance network or detect any improper conduct., they can leave at any round, thus ensuring QoS and addressing the limited oversight of off-chain operations in distributed systems.

② By utilizing the concept of multiple interactions, the framework eliminates the relatively complex process of establishing trustworthiness and provides faster network service. Furthermore, it reduces access latency and brings more immediate and efficient service by allowing the subject to provide service before the smart contract is uploaded to the blockchain network.

③ Since clients do not need to establish trustworthiness with the subjects in the alliance network in advance, the framework is more flexible compared with conventional schemes. Therefore, it enhances the trustworthiness relationship between clients and subjects and also incentivizes cooperation between both sides without relying on trusted third parties, thus facilitating the efficient handling of high-frequency service establishment requests and tackling the problem of surging demands in the alliance network.

(2) Blockchain-based Network Layer Solution

Blockchain security significantly depends on consensus nodes. However, the challenge is magnified in communication networks due to device diversity, data heterogeneity, and complexity, complicating the assurance of consensus node reliability. The risk of malicious base stations blocking information spread necessitates Byzantine Fault Tolerant (BFT) protocols for owner network layer dissemination, aiming for efficient, universally trusted networks. Traditional Practical

Byzantine Fault Tolerance (PBFT) protocols face scalability issues in networks with many base stations. A dual-layer blockchain consensus approach overcomes these issues, better aligning with the needs for fast consensus, parallel processing, high throughput, low latency, cost-efficiency, scalability, and security in communication networks.

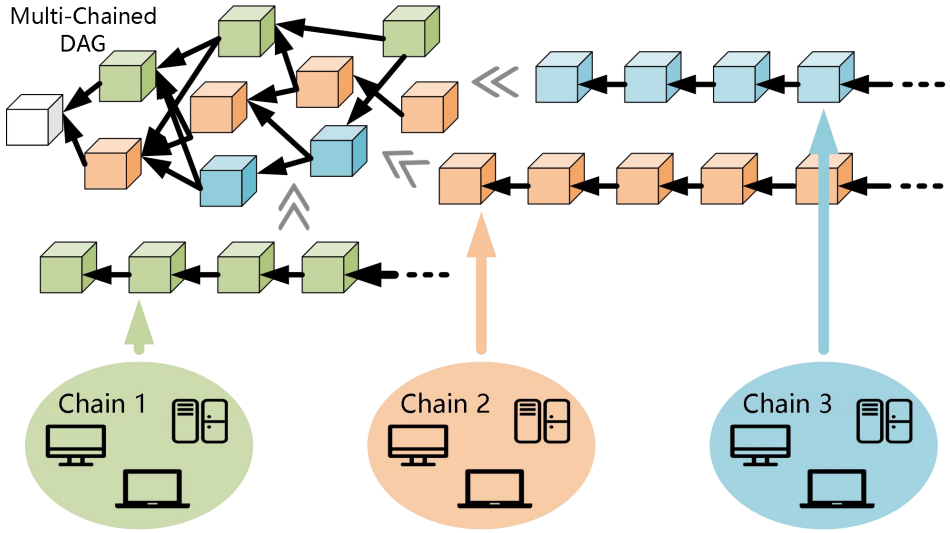

Figure 5-4: Structure of DAG-based cross-chain collaborative CM

Figure 5-4 illustrates the cross-chain collaboration consensus structure based on the Directed Acyclic Graph (DAG) blockchain. The Chain 1, Chain 2, Chain 3 represent an independent local blockchain system which can be constructed in A1, O1, O2, E2, F1-c, F1-u, CUS-Plane and M-plane. Besides, the number of local chain system should be predetermined to prevent generation of malicious local chain system. Through partition independence and cross-layer collaboration, this approach achieves an effective integration with communication networks. By ensuring security, privacy, and resource slice independence at the base layer, it addresses the decentralization needs of a universally trusted network without overly simplifying the complexity involved through two layers of the consensus: DAG-based cross-chain collaborative consensus and independent consensus in the local blockchain system.

① Layer 1: PoW-based block generation consensus mechanism

Every node in the whole blockchain system will generate and receive transaction information only in the local chain system. For example, a node in Chain1 blockchain

system can only receive transaction information within Chain 1, not from Chain 2 or other independent local blockchain system. When blockchain nodes receive transaction information, it will verify transaction legitimacy by verifying transaction completeness and transaction validity. When transaction verification failed, it will not be packaged into new block. During the verification, the blockchain node tries to solve a PoW problem which co-proposed by local chain system information (used to adjust block generation rate) and blockchain difficulty information (used to assure that PoW problem difficulty level is same for each local blockchain system and assure that PoW problem is different for new block). The first node that solved PoW problem can broadcast the new block with the successfully verified data set.

② Layer 2: DAG-based cross-chain collaborative consensus

- Step 1: If a node generated a new block, the node will be awarded with certain weight (say 1) and the node needs to verify two different blocks (call it head) that with weight 1 (this information stored locally in DAG ledger) for the block legitimacy and cross-chain transaction verification.
- Step 2: When verification passed, the block will broadcast to the global blockchain nodes.
- Step 3: The new block in local blockchain system is now as the head in the blockchain system, which wait for verification by node in other blockchain systems.
- Step 4: Only a transaction is legal globally when the accumulated weight meets the threshold of the consensus.

Note: The weight in DAG is accumulated by the number of blocks that generated afterwards. Due to the “longest chain” rule, which is the transactions in the longest chain blocks is legal globally, malicious forks (diverges mainchain into two blockchains with an honest chain (where the chain is expanded by honest nodes) and a malicious chain) require computing resources larger than 51%.

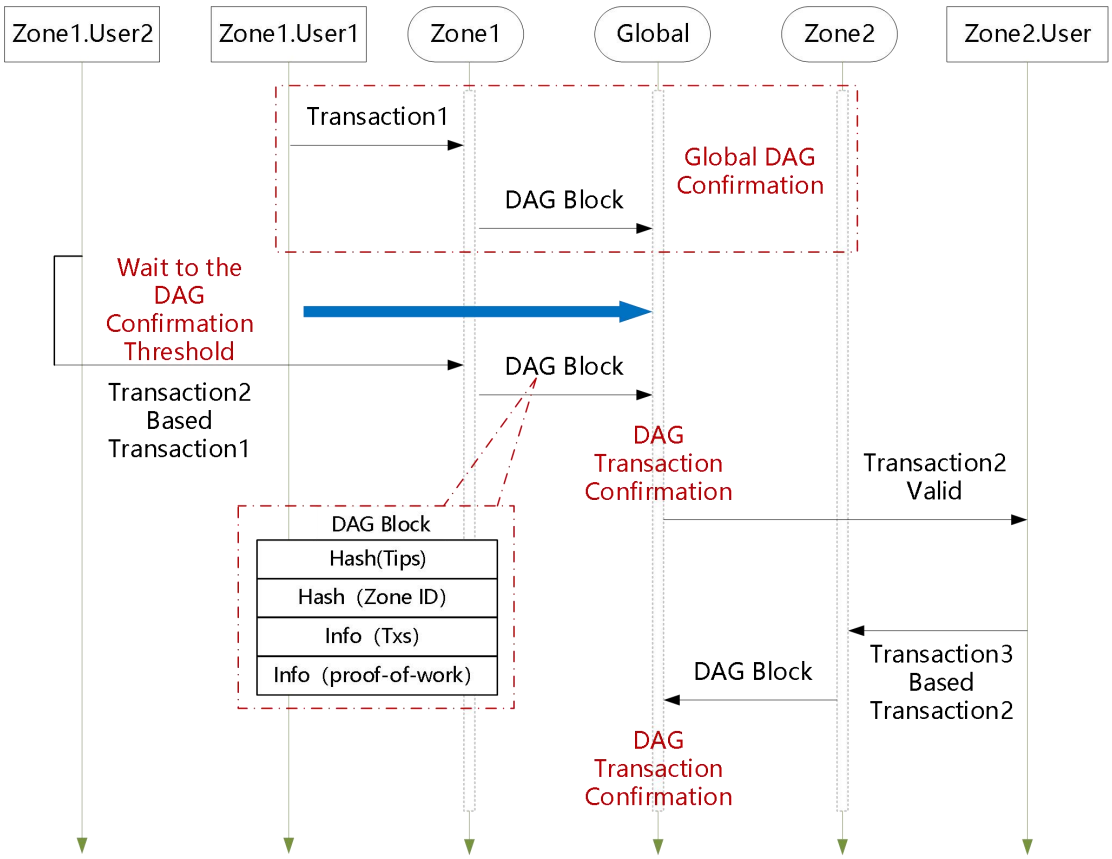

Figure 5-5 Cross-chain transaction confirmation process

Figure 5-5 shows the cross-chain transaction confirmation process, where Chain 1 User lunch transaction with Chain 2 User. It shows that the transaction information in independent blockchain systems will broadcast to the blocks in that system. Besides, Transaction lunched by Chain 1 User or lunched by Chain 2 User is the same in the scope of transaction confirmation process. It also shows that different layers have connections to achieve cross-chain collaborative consensus. To reduce the effect caused by interconnection, this consensus mechanism verifies cross-chain transaction and ordinary transaction in different way. Cross-chain transaction verification is distributed to all the interconnected nodes in the global blockchain system, which greatly improves the difficulty of double spending on cross-chain transaction. Verification of cross-chain transaction is a supplement for ordinary transaction verification original blockchain system. By this method, it can collaborate blockchain system and ensure that each local blockchain system keep its independence.

6. Conclusion and Outlook

Einstein once said: A problem cannot be solved from the level that causes it to arise. After decades of development, the industry generally believes that in the 6G era, mobile communication networks need to rise to higher dimensions in order to open up new business spaces and expand customer base, create new growth points and business models. The consortium network has emerged, which organizes networks belonging to different owners (such as ground and satellite operator networks, government, enterprise and industry networks, households and personal networks) together. Through interconnectivity, trustworthy security, and right protection, it forms an ecosystem where resources, functions, and services can be shared and traded with each other. While reducing resource acquisition costs, it increases monetization capabilities, creating a lighter and more cost-effective, higher-return on investment and more ubiquitous network infrastructure.

The ecosystem of consortium networks cannot be achieved overnight. Although this white paper is called the consortium network system and architecture white paper for 6G, it does not mean that it is necessary to wait for 6G to start the technology and industrial practice of consortium networks. In fact, in recent years, relevant practices on a global scale have been constantly evolving. The domestic IMT2030 has conducted discussions and tests on the architecture of distributed owner networks and blockchain trusted networks. In Europe, there are architecture designs represented by subnets/networks of networks, and in the United States, there are commercial practices represented by HELIUM that combine WEB3 and wireless communication networks. These practices provide some early validation of relevant technologies or business models for the consortium network. Based on this, the consortium network can rebuild its system and architecture and embark on a more stable, feasible, and consensus based development path.

As the world's first white paper titled consortium network, this white paper only covers the basic concepts, value scenarios, core features, system and architecture, and

key technologies of consortium network. The purpose is to introduce consortium network to telecommunications industry practitioners and non telecommunications industry partners, and invite experts and scholars from industry and academia to join the ecosystem of consortium network, continuously improve the business and technical system of the consortium network, and promote its continuous evolution towards maturity.

Abbreviation in the Paper

Abbreviation	Full name
ODICT	Operation Data Information Communication Technology
KPI	Key Performance Indicator
KVI	Key Value Indicator
KDI	Key Development Indicator
ToB	To Business
AI	Artificial Intelligence
DID	Decentralized Identity
DNMF	Distributed Networks Management Function
NRF	Network Repository Function
SCP	Service Capability Exposure Function
MNO	Mobile Network Operators
PKI	Public Key Infrastructure
CA	Certificate Authority
NF	Network Function
IS	Identity Subject
SBA	Service-based Architecture
QoS	Quality of Service
PBFT	Practical Byzantine Fault Tolerance
DAG	Direct Acyclic Graph
PoW	Proof of Work

Participant：

No.	Participant	Main Contributor
1	ZTE Corporation	XIE Feng、ZHANG Kangjie、HUANG Fenghe、XUE Yan
2	China Telecom Research Institute	LIN Yilin、LIU Jie、CHEN Sibai
3	Beijing University of Posts and Telecommunications	CAO Bin、LIU Jiashuo、LI Haoyang
4	Southeast University	LING Xintong、CHEN Shiyi、HU Jingxiang
5	CICT Mobile	CHENG Zhimi、LI Huixin
6	China Unicom Research Institute	LIANG Tingting、SUN Mingrui
7	VIVO	JIANG Dajie