An study on the application of blockchain based 5G Technology in the Power IoT

WANG Dan[1*], ZHAO Xunwei[1], BAI Jie[1], WU Qing[1], WANG Wenhua[1]

[1] Research Institute, State Grid Information & Telecommunication Group Co., Ltd., Beijing, 100052, China

Abstract. Based on some key characteristics of 5G and blockchain, we analyze the technical feasibility and necessity of combining 5G and blockchain in IoT construction. We prove that the combination of 5G and blockchain can effectively improve network and data security of 5G by discussing the practical problems that can be solved by this method(including distributed deployment of network platforms, slicing management, network security authentication, spectrum resource management, data sharing security), while moderately reducing network complexity. Finally, we discuss the application of 5G and blockchain combined technical architecture in the construction of the Internet of Things (IoT), focusing on the requirements of power transmission, substation, distribution and consumption. We analyze the 5G network slicing management based on blockchain technology, which can realize the dynamic selection of the best resources among multiple resources to create end-to-end network slices that meet business needs and security isolation requirements, and enhance the security of the network and the data in multiple scenarios and applications, it will provide a strong network infrastructure support for the Energy IoT service system.

1 Introduction

Grid-oriented application scenarios, along with the continuous transformation of energy production and consumption structure, grid construction and power applications will continue to deepen. "grid control" will spread to the end and the whole processing, making "information data" grow explosively. 5G technology is needed to provide a High-security, low-latency, large-bandwidth, high-reliability, and large connectivity communication services to improve and innovate the deeper perception capabilities of the power grid business in all scenarios[1]. At present, State Grid and NNCC have been actively promoting 5G application research and landing in business scenarios such as precise load rapid control, differential protection of distribution networks, massive micro-load participation in flexible grid control and auxiliary services, precise governance of operation and distribution data.

Among these application scenarios, the security of 5G, as an important method of access to power communication networks, is very important[2]. And blockchain is an information security technology known for its security.So 5G and blockchain, as the state-in-art technology in their respective fields, have very broad prospects for cooperation. The combination of blockchain technology, deploying at the edge with Peer to Peer (P2P) networking with self-executing scripts and consensus mechanisms to enhance the security policy of 5G networks, can provides a new set of solutions for 5G networks and services. It can enhance the security, privacy and decentralization of date, and improve network management architecture, thereby improving the quality of user services (Quality of Service, QoS), and ultimately ensuring the secure operation of the power IoT.

2 Technical Feasibility Analysis of the Combination of 5G and Blockchain

The development of Internet of Things (IoT) will inevitably leverage some features of 5G networks, such as the large connectivity, high reliability and ultra-low latency, to support the those needs, including huge number of IoT device connections, large scale data frequency, big data and artificial intelligence applications[3]. However, as the necessary conditions for the successful development of the Internet of Things industry are "Internet of Everything, Security First", we need to combine the distributed, non-tamperable, traceability, transparency and high privacy of the blockchain to realize the storage and management of 5G data, and Optimize the 5G network to enhance the security of the 5G ecosystem and better adapt to the needs of IoT[4].

2.1 distributed deployment

In the 5G era of multi-cloud and hybrid cloud scenarios, especially for the power grid industry, where application workloads are complex and business coverage is extensive, centralized and distributed architectures are no longer an "one or the other" choice. When multiple users request data or server response at the same time, the centralized

*Corresponding author's e-mail: wangdan2@sgitg.sgcc.com.cn

system cannot guarantee The service will not be interrupted due to software errors or other reasons. For example, if the cloud computing model relies on a centralized service provider, it is vulnerable to the threat of a single point of failure, which in turn affects the availability of cloud services. When multiple users request data or server responses at the same time, a centralized system cannot guarantee that services will not be interrupted due to software errors or other reasons[5]. The blockchain protocol is vertically divided into application layer, contract layer, consensus layer and network layer, and except for the applicaton layer all the other layers can be distributed and deployed in different network locations. Based on the unique structure of the blockchain, the distributed deployment of the platform can be achieved, eliminating the centralized control of the core network.

By using blockchain technology, the number of centralized control servers can be reduced in the building of a 5G network, and service delivery can be achieved through blockchain, such as user access control, service response, etc., which can be implemented in a distributed database, eliminating the need for additional management structures.

2.2 Network Slice Management

5G network slicing means dividing the network into multiple sub-networks, such as through Network Function Virtualization (NFV), to provide customized network services for different work scenarios[6]. Since end-to-end services may deploy NFV in multiple service provider environments, different users usually need to share the same cloud infrastructure, which is vulnerable to internal attacks, and any problems in any one link can lead to security issues such as data leakage.

As shown in Figure 1, using blockchain technology to include information such as bandwidth, channel power and data rate in each record of the virtualized slice and make it available to users at the time of service, and such transactions are immutably recorded in a shared block, the concept of blockchain ledger is used to add a ledger management layer to the slice management to enable autonomous and dynamic allocation of slices. When an operator receives a request or query to establish a slice, it submits the request to the blockchain layer for tracking and sharing, and supports the deployment of sub-slice components through self-executing scripts, with different scripts corresponding to different slice resources. In this way, the resource side can perform resource transactions on contracts with sub-slice components. All information about sub-slice management is logged in a licensed blockchain controlled by the operator, which not only increases the security capabilities but also supports a problem backtracking mechanism.

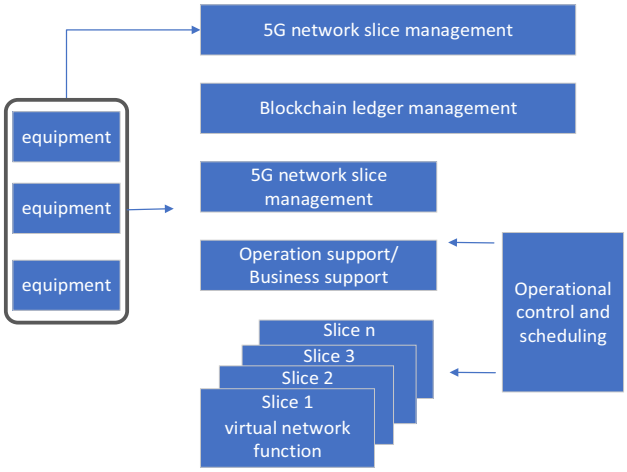

Figure 1. Blockchain for the Management of 5G networks slice

2.3 Network Security Certification

In terms of 5G network security authentication, unlike conventional database management systems that typically use centralized servers to enforce access authentication and security mechanisms, blockchain networks can enable distributed user access authentication by mobilizing the computing power of all legitimate network nodes[7][8]. This makes functions such as spectrum sharing, data sharing, and resource allocation easier to implement, and makes it easy to detect attempts by illegitimate nodes to disguise and tamper with data. At the same time, with the support of intelligent self-executing scripts, blockchain can provide flexible and efficient user access control mechanisms through access rules and predefined logic, resulting in a blockchain-based authentication solution for 5G networks. Intelligent executable contracts do not need to rely on external security authentication support and can automatically authenticate user access without revealing user information, detect threats and block malicious access, while publishing user data to a distributed database, where the data is extremely secure due to the existence of block data structures. Under extreme conditions, blockchain can provide complete control and traceability mechanisms over data when it is shared across untrusted networks, which is difficult to achieve with all traditional methods.

2.4 Network System Performance

By reaching a control protocol through blockchain consensus, the computing power of all nodes can be used to manipulate the network instead of being based on a few core nodes or third party organizations, finally it can establish secure P2P communication between users and even directly support D2D (Device-to-Device) communication[9]. These functions will reduce communication delays, reduce costs, and provide global secure access for all nodes. Even if individual nodes are under malicious attack, the network as a whole can continue to operate based on consensus mechanisms and intelligent executable scripts. Isolation of faulty nodes ensures that no single point of failure will cause data

loopholes or system crashes, enhance overall system performance and increase trustworthiness.

For example, D2D communication in 5G networks is realized through a P2P network established by the blockchain. As shown in Figure 2, As shown in Figure 3, each D2D device is converted into a node in the blockchain network, and the blockchain records of exchanged data are stored on some or all nodes. Blockchain records, can be used to verify and monitor data at any time, and can be traced back at any time, which can achieve better system transparency and reliability. Moreover, based on the P2P architecture, the communication between 5G service providers and actual users is more direct, which is conducive to reducing operation, maintenance and management costs, which makes 5G systems more flexible and efficient in delivering data while ensuring security.

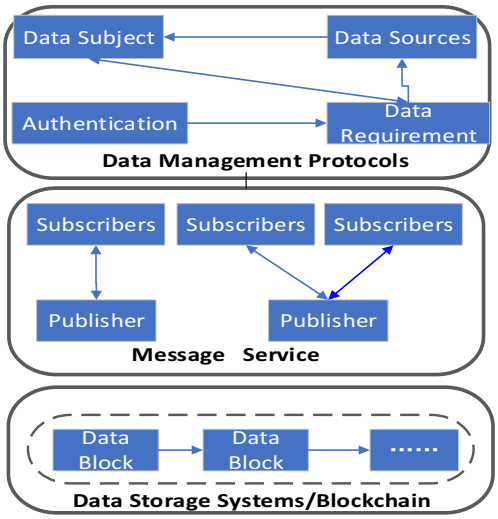

Figure 2. Blockchain for Accese Control of P2P

In addition, compared to traditional database platforms such as SQL, blockchain can provide better data storage and management services through low-latency data retrieval. For example, resource requests or data access can be completed by accessing decentralized blockchain nodes and verified by intelligent executable scripts, without the need for centralized authorization through core nodes, greatly reducing network latency.

2.5 Overview of the Key Technology research on the combination of 5G and Blockchain

Blockchain can be tightly connected to 5G technology as described in Sections 2.1-2.4, and the underlying database can be built in a data center or in various nodes in a 5G network, such as base stations, edge devices, or even end devices. Taking the architecture of the Open-Radio Access Network (O-RAN) as an example[10][11], the central unit (Center Unite, CU) part of the Base Band Processing Unit (BBU) can be integrated with the core functionality of the blockchain to generate and manage the blocks. In the non-Real Time (non-RT) layer of the RAN Intelligent Controller (RIC), it is necessary to complete network management, online learning and offline training of AI models, as well as deployment functions, strategy selection and issuance. Those issues can be achieved through the consensus mechanism of the blockchain and recorded through the blockchain. In the near real-time layer (RIC Near-Real Time (Near-RT)) of the RIC, work such as bearer control, control delay, wireless connection management, mobile management, UE-level load balancing, QoS management, interference management, scheduling strategy and slicing optimization, etc., can be achieved through self-executing scripts on the blockchain and recorded in the blockchain for easy operation and maintenance as well as backtracking.

In summary, the combination of blockchain technology and 5G technology can effectively reduce network complexity and save a lot of operating costs. 5G network services, such as data sharing, spectrum sharing, etc., can be directly controlled by the blockchain network[12]. Based on the consensus mechanism, all nodes or some nodes can be authorized to have the authority to manage and maintain the network, and the authority between authorized nodes can be equal or different, according to different needs and application scenarios, which can be adjusted flexibly at any time. Using blockchain technology, it can also fully leverage the capabilities of nodes within the 5G network, such as computing and storage capabilities, fully complementing edge computing and cloud computing, simplifying the organization and management of the network, providing a better user experience, and adapting to the complex mobile environment of future 5G networks, especially in some complex vertical application scenarios.

3 Exploring the combination of 5G and Blockchain in the power industry

The electric power communication network is an important infrastructure of the electric power system. A large number of widely distributed business terminals and communication terminals are deployed. The security of its data relates to the safe and stable operation of the entire power grid[13]. 5G supports the ubiquitous, convenient and efficient connection of the Power Internet of Things (PIoT) and the expansion of new services, and the blockchain supports the data integration, secure transmission, operation and maintenance management of the PIoT.

As shown in Figure 3, all layers in the blockchain can be closely connected to the common 5G network, and the underlying database can be built in the data center or in various nodes in the 5G network, such as base stations, edge devices, and even terminal devices. On the edge side, data from the smart grid and smart IoT can pass through certain blockchain servers to perform point-to-point transmission and data recording functions, and can respond quickly to specific situations based on consensus predefined schemes. On the core network side, blockchain services can be combined with the core functions of 5G to perform functions such as encrypted communication between NFV modules and network slicing policy settings.

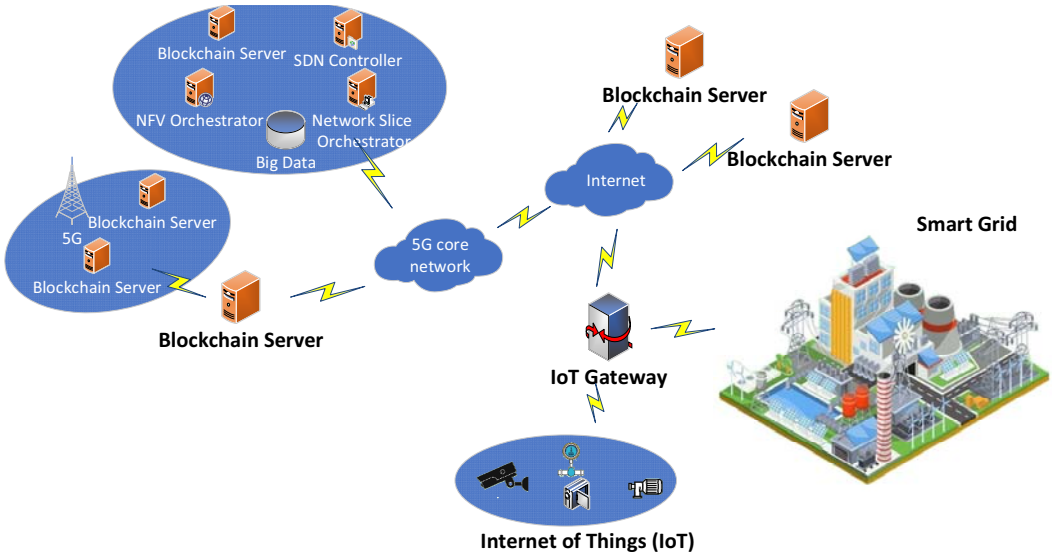

Figure 3. The Convergence of 5G and blockchain in the Power Internet of Things

For example, in the transmission section, line status monitoring and drone inspections, based on the reliable communication platform for status information and inspection information through 5G networks, can use blockchain security mechanisms to establish a distributed, point-to-point security delivery mechanism to ensure the accuracy of information and transmission, and to record monitoring and inspection results in real time. In the substation section, such as the substation intelligent inspection, blockchain-based 5G technology can be used to access control and scheduling of monitoring equipment, encryption and storage of monitoring data, preventing someone from maliciously intruding into the monitoring network, controlling monitoring equipment, or stealing monitoring information, which may cause heavy losses. On the distribution side, blockchain-based 5G applications will be more extensive, covering the whole process from fault monitoring and location to precise load control[14][15]. These applications have very high requirements for low latency, and the number of connections that need to be managed is also relatively large, basically in the millions and tens of millions, while the distributed technology of blockchain can just solve this problem. The failure of some nodes will not affect the operation of the overall network. And the blockchain can be easily deployed on the edge to reduce latency. At the power consumption end of the grid, there are a large number of nodes, involving power information collection, charging piles, smart home and other energy measurement or power management applications, etc. Using 5G networks to achieve large connections and data collection, combined with blockchain technology, can protect data privacy and detect abnormal situations. If there is data tampering, a forked chain will be formed, which is easy to locate abnormal data nodes.

Taking the power dedicated network slicing as an example, it is an ideal choice for realizing 5G power applications, which can be flexibly customized with different network functions, different security isolation degrees and different Service Level Agreements (SLA) to guarantee a specific sub-network, according to the different needs of multiple services in the grid. For 5G slicing grid applications, an intermediary mechanism based on blockchain to deploy the sub-slices can be designed[16]. A series of contract scripts with unique identifiers and data fields can be used to create new contracts or update the state of the blockchain. Each of the sub-slice in the network corresponds to the contract script in the blockchain. When the contract script and the corresponding sub-slice have completed the negotiation and confirmation, the end-to-end slice deployment can be started. Figure 5 describes the process of creating 5G network slice based on blockchain in power grid applications. Resource Pool (RP), which can be radio resources (eNB, CU, DU, RRU, MAC scheduling algorithm, etc.), compute resources (such as CPU, the number of virtual machine instances, etc.), storage resources, transport resources (VPN, VLAN, bandwidth, wait time, etc.), is a collection of resources available for slicing. A slice may contain multiple RPs.

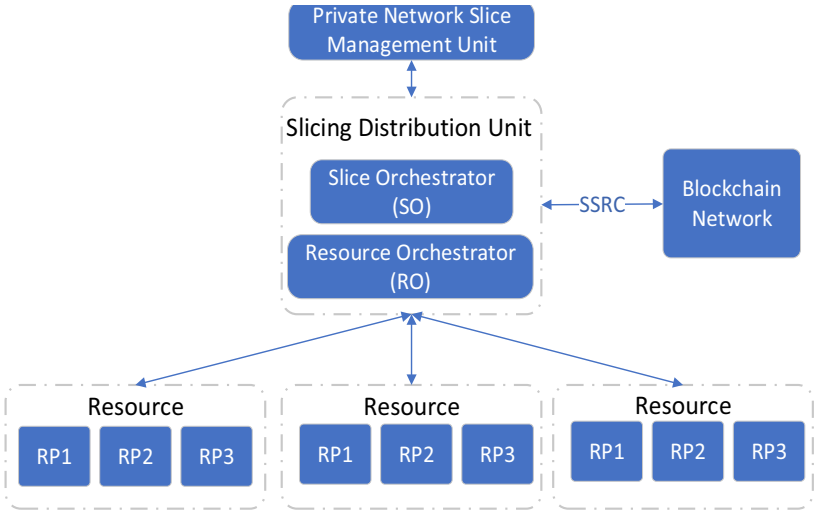

Figure4. The Process for creating 5G network slices of the power grid based on blockchain

Create Slice template: the slice manage- ment unit requests a template to create slices.

- Define resource pool requirements: the slice allocation unit converts the template into a specific slice resource requirement, such as the number and the type of sub-slices, virtualized network elements, physical network elements, and physical resource requirements.
- Blockchain-based sub-slice requests: the corresponding sub-slice requests are made through the blockchain network. Each sub-slice request will generate a negotiable contract script. When the request query reaches the blockchain network, the blockchain network will create and publish a sub-slice resource contract (Sub-Slice Resource Contract, SSRC). The SSRC specifies the necessary resources required for the sub-slice and the duration of the service.
- The cost of publishing slice deployment by the resource party: since all resource contracts are visible on the blockchain, the resource party can respond by publishing a sub-slice deployment cost message, which indicates the cost of the sub-slice component provided by the resource party.
- Resource selection and slice deployment: the original SSRC collects cost messages from all resource parties and arbitrates to select a resource party to deploy sub-slice components based on specific objectives (such as delay, bandwidth, etc.), and the slice orchestrator SO will use the resource orchestrator RO interface to instantiate and create sub-slicing to build end-to-end network slices.
- Supervision of slice quality: all relevant information about the slice deployment is recorded in the permission blockchain managed by the slice allocation unit. The resource owner uses its RO interface to manage and coordinate its resources ,and exposing the interface will allow other ROs or SOs to interact with the local RO. The RO provides monitoring information about the resource usage of the relevant sub-slices for the slice allocation unit to verify whether the agreed resource party meets the target SLA.

In 5G power applications, by adding business entities such as slice allocation management that combined with blockchain technology to record and manage slice resource allocation, it is possible to achieve dynamic selection of the best resources among multiple resource parties to create end-to-end network slices that meet business needs and security isolation requirements, and improve the overall performance of 5G networks that carry power services. At the same time, the blockchain-based slicing architecture achieves the same isolation and security guarantees as the private network. Compared with the construction of a dedicated optical network, the construction cost is greatly reduced.

In general speaking, all aspects of power grid operation, from line inspection, equipment room management, fault isolation to intelligent dispatching, can make full use of the technical architecture of the combination of 5G and blockchain to establish a highly secure power 5G wireless communication network, while through self-executing scripts and distributed deployment for slicing and scheduling at the edge, we can reduce service latency, realize real-time collection and sharing of massive power equipment monitoring and other data, and help realize the Power IoT.

4 Conclusions

The exploratory application of the combination of blockchain and 5G in the Power Internet of Things will form a good demonstration and promotion effect, effectively solve the problems of data integration, device security, personal privacy, and multi-subject collaboration faced during the construction of the Power IoT. How to reconstruct 5G and blockchain technology to form an architecture that is deeply integrated with the power system is the main development direction for the integration of 5G, blockchain and energy systems in the future. "5G + blockchain + smart energy" will be a new form of energy industry development which base on the 5G communication network and blockchain, that

integrating the energy production, transmission, storage, consumption and energy market.

References

1. M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.
2. N. Panwar, S. Sharma, and A. K. Singh, “A survey on 5G: The next generation of mobile communication,” Physical Communication, vol. 18, pp. 64–84, 2016.
3. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions,” IEEE Communications Surveys & Tutorials, 2019.
4. A. Gupta and R. K. M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H.Rehmani, “Applications of blockchains in the internet of things: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2018.
5. ZYSKIND G, NATHAN O. Decentralizing privacy: Using blockchain to protect personal data[C]//IEEE Security and Privacy Workshops, San Jose, CA, USA. Piscataway, IEEE Press, 2015: 180-184.
6. DORRI A, STEGER M, KANHERE S, et al. Blockchain: a distributed solution to automotive security and privacy[J]. IEEE Communications Magazine, 2017, 55(12):119-125.
7. DORRI A, KANHERE S, JURDAK R, et al. Blockchain for IoT security and privacy: the case study of a smart home[C]// IEEE International Conference on Pervasive Computing and Communications, March 13-17, 2017, Kona, HI, USA. Piscataway: IEEE Press, 2017: 618-623.
8. KARAVAS C S, ARVANITIS K, PAPADAKIS G. A game theory approach to multi-agent decentralized energy management of autonomous polygeneration microgrids[J]. Energies, 2017(10): 1756.
9. LIU N, YU X, WANG C, el al. An energy sharing model with price-based demand response for microgrids of peer-to-peer prosumers[J]. IEEE Transactions on Power System, 2017, 32(5):3569-3583.
10. Zhang Jianqiang, Zhang Gaoyu. Analysis of the application of blockchain technology in the Internet of Things[J]. Telecommunications Science, 2018, 34(S1): 104-110.
11. Zhao Minghui, Zhang Yu, Qi Jin. Blockchain-based Trusted Service Management Framework for the Social Internet of Things [J]. Telecommunication Science, 2017, 33(10): 19-25.
12. Zou Jun. Blockchain technology guide [M]. Beijing: Machinery Industry Press, 2016.
13. Niu Danyang. Research and Implementation of Blockchain-Based Electricity Safety Protection Technology [D]. Beijing: Beijing University of Posts and Telecommunications,2019.
14. SIEBERT L C, FERREIRA L R, YAMAKAWA E K, et al. Centralized and decentralized approaches to demand response using smart plugs[C]//T&D Conference and Exposition, April 14-17,2014, Chicago, USA. Piscataway: IEEE Press, 2014: 1–5.
15. Yuan Yong, Wang Feiyue. Blockchain technology development status and outlook[J]. Journal of Automation,2016, 42(4): 481-494.
16. G. H. Carvalho, I. Woungang, A. Anpalagan, and M. Jaseemuddin, “Analysis of joint parallelism in wireless and cloud domains on mobile edge computing over 5G systems,” Journal of Communications and Networks, vol. 20, no. 6, pp. 565–577, 2018.