Design and Development of a BaaS System Based on Intelligent Scheduling and Operation Cloud-Edge Platform

Yaping Hu, Yiqian Lin, Yongquan Nie, Chaoyi Peng, Yubin He, Yuxuan Liu, Guang Ma, Dewen Seng

Abstract—**As China's electricity market continues to evolve, the increasing number and diversity of market participants have led to a rapid increase in data volume. An immediate challenge is designing a robust blockchain system that ensures not only the transparency, credibility, tamper-resistance, traceability, privacy, and security of substantial market data in a complex environment, but also provides trusted data support for intelligent dispatching within the power market. This paper proposes a solution to this pressing issue through Blockchain as a Service (BaaS). BaaS leverages the capabilities of cloud computing platforms to enhance the ease and efficiency of deploying and operating blockchain systems. Specifically, the paper introduces a BaaS system built upon an integrated intelligent scheduling and operation cloud-edge platform (CEP). It incorporates technological solutions such as data on-chain, trusted comparison, edge cluster data transmission, optimized transaction authentication, and lightweight storage nodes. Rigorous testing has conclusively demonstrated that the proposed BaaS system meets the requirements of the digital transformation of the China Southern Power Grid, and provides robust technical support for its future practical applications.**

Index Terms—**Blockchain, Blockchain as a Service, Cloud computing, Electricity market**

I. Introduction

With the influx of numerous market participants, there has been a significant rise in the development of distributed energy, opening up new opportunities within the electricity market. However, this growth has also brought about unprecedented challenges.

Firstly, the integration of a multitude of market entities into the electricity market system has led to an explosion of information and data. This not only escalates the complexity of verifying the credibility of this extensive data but also places higher demands on the resources and operational costs of the electricity system. Furthermore, it necessitates the development of new functions for data verification [1].

Secondly, the diverse system environments of the market participants pose additional challenges. Some participants may be constrained by low network bandwidth or limited computing and storage capacities. Existing blockchain systems, which consume significant network, computing, and storage resources, exacerbate these challenges. Therefore, our new system needs to possess the flexibility required to adapt to these varied and complex environments.

The integration of cloud computing and edge computing effectively manages the computation and storage of extensive data. Previous research has explored the advantages of blockchain technology in establishing data trust mechanisms [2-8], as well as its application in conjunction with edge-cloud synergy in distributed energy trading systems [9]. However, these studies only partially address the problem. Current research on ensuring the transparency, credibility, tamper-resistance, traceability, privacy, and security of data in complex system environments is still limited.

In response to these challenges, this paper proposes a Blockchain as a Service (BaaS) system [10-12] based on intelligent scheduling and a cloud-edge operational platform [13, 14]. This paper provides an in-depth analysis of various system architectures, and offers detailed descriptions of core technical solutions, including trusted data on-chain, trusted data comparison, edge cluster data transmission, optimized transaction authentication, and lightweight storage nodes. In conclusion, the BaaS system demonstrates excellent environmental adaptability and meets the data credibility requirements of the electricity market.

II. Construction Principles

A. Design Principles

The construction of the BaaS system strictly adheres to the following design principles:

(1) High reliable: The system adopts technologies such as cluster, virtualization, disaster backup, load balancing, multiple replica redundancy, data backup, and data recovery to eliminate single point of failure and ensure reliable data security and service continuity. Multiple copies of each data

Manuscript received September 11, 2023; revised December 26, 2023.

Yaping Hu is a professor level senior engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: huyp@csg.cn)

Yiqian Lin is a postgraduate student of School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China. (e-mail: linyq@hdu.edu.cn)

Yongquan Nie is a senior engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: nieyq@csg.cn)

Chaoyi Peng is a senior engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: pengcy@csg.cn)

Yubin He is a senior engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: heyb1@csg.cn)

Yuxuan Liu is an engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: liuyx10@csg.cn)

Guang Ma is an engineer of Power dispatch and control Center, China Southern Power Grid, Guangzhou 510623, China. (e-mail: maguang@csg.cn)

Dewen Seng is a postgraduate tutor and assistant professor of School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China. (Corresponding author, e-mail: sengdw@hdu.edu.cn)

are maintained, allowing for swift recovery in the event of single data corruption [15-19].

(2) High safe: The system's functional modules adhere to information system security level protection requirements (the portion deployed in the cloud system follows security level 3 standards, while the part in the edge cluster follows security level 4 standards) and the relevant standards and norms of power secondary system security protection. Through the pre-launch grade protection evaluation, security assessment source code audit work.

(3) Extensible: The expansion of system's functional modules, such as lateral expansion, program upgrades, the addition or removal of service nodes, can be seamlessly executed online without disrupting existing functionalities. Additionally, it possesses forward compatibility, ensuring that historical models, graphics, and data can continue to be utilized even after program upgrades.

(4) High available: The application services of the platform's function modules embody characteristics such as immediate availability, on-demand upgrades, transparent compatibility, and convenient management.

(5) Compatible: The platform can operate smoothly on PC servers using either ARM or X86 CPU architecture. It supports hybrid deployment on underlying physical servers that are compatible with multiple chip architectures. Application interactions are compatible with both IPv4 and IPv6 technologies.

(6) Multi-user: The platform enables concurrent access by multiple users, maintaining consistent performance even during simultaneous usage. Different users' operations and configurations are isolated from one another, and the generated data is stored separately to prevent interference.

(7) Adaptation to resource-constrained environments: The platform ensures compliance with on-chain performance requirements even in scenarios with limited bandwidth, storage, and computing resources.

B. Security Metrics

The BaaS system must meet the following safety criteria, including:

(1) Encryption of transmitted data during network transmission;

(2) Ensuring resistance to intrusion, attacks, viruses, leaks, tampering, repudiation, phishing, and other security threats;

(3) Implementing permission management for system operation functions.

III. System Architecture Design

As an increasing number of market participants access, relying solely on the traditional cloud computing model has been insufficient for efficiently process the data generated by various distributed devices. It also fails to meet the requirements for transparent and credible data from market participants. To align with the operational characteristics of China Southern Power Grid and transition from a centralized model to an open, shared, and intelligent interaction approach, China Southern Power Grid has formed a "cloud" brain + edge node cloud edge fusion architecture of two-stage synergy. As part of this architecture, some data processing tasks from the cloud system [20, 21] are offloaded to edge nodes, reducing the resource demands on the cloud system. These edge nodes including edge cluster systems [22] and edge gateways [23]. Within the new power system, the edge cluster system centrally manages the subordinate edge gateways, transmitting edge node data to the cloud system and receiving instructions from it. The edge gateway serves as an integrated device deployed within the distributed electricity market participants' environment, facilitating plug-and-play access to the edge cluster system for receiving control instructions and acting as an entry point for accessing data from numerous equipment objects.

In order to satisfy the requirements for transparency, trustworthiness, tamper-proof, traceability, privacy and security of massive market entities' data within the cloud-edge integration ecosystem, blockchain modules are deployed across cloud systems [24], edge clusters, and edge gateways. Simultaneously, recognizing the formidable performance demands associated with handling extensive data access within a single blockchain network, the substantial resource prerequisites for an individual node, and the necessity of maintaining data privacy and security in the intricate blockchain network environment, this paper presents a multi-chain architecture.

A. Overall Architecture

The overall system architecture comprises four main components: the cloud system, edge cluster, edge gateway, and aggregation subject platform. Within this architecture, the blockchain platform function modules are deployed in the cloud system to realize the comprehensive monitoring of blockchain operations across the entire grid, as well as the secure storage and utilization of trusted data throughout the entire grid. Moreover, a Blockchain as a Service platform (BaaS) is deployed within each edge cluster, offering visual blockchain alliance governance functions to cluster users. When a new affiliate aggregation subject access, they can request dynamic BaaS blockchain resources. If jurisdiction over the edge of a cluster multiple polymerization, a new blockchain distribution channel is created for aggregation subjects, and by default, the edge cluster is included in each channel. Additionally, the edge cluster also provides data file transfer service across distinct secure zones. The edge gateway serves as an all-in-one device, integrating blockchain nodes and deployed at the aggregation subject's side, serving as the entry point for data from detection terminals connected to the chain. The blockchain nodes deployed on the aggregator platform, along with the blockchain nodes on the edge gateway and edge cluster, collectively form a blockchain network, participating in blockchain consensus mechanisms. The overall architecture diagram is depicted in Fig. 1.

The direct interaction system encompasses various components, including but not limited to:

(1) Monitoring Terminal: Collect equipment operation data, accurate to the second level, and send the data to the blockchain network within a specified time interval.

(2) Aggregator Platform: Participate in the blockchain consensus and receive the consensus ledger data. The aggregator platform will also transmit the aggregated processed power data to the edge cluster, which will collect this part of data as one of the trusted comparison sources of blockchain data.

(3) Edge Gateway: Pre-installed blockchain nodes serve monitoring terminals within the aggregation subject's jurisdiction, receive their on-chain requests, and synchronize the on-chain ledger data with other blockchain nodes.

(4) Edge Cluster: Receive the aggregation data reported by the aggregation subject platform within the cluster's jurisdiction and the data directly collected from monitoring devices through the blockchain node in BaaS. The blockchain operation data, aggregated data and device direct data are transmitted to the cloud system through a trusted channel.

(5) Cloud System: Deploy blockchain platform functions, receive blockchain operation data from the entire grid and aggregating electric data and equipment direct collection data, to realize blockchain operation monitoring and trusted data storage and utilization for the entire grid.

Through this hierarchical multi-chain design, it not only achieves data isolation, but also significantly reduces the requirements for blockchain resources, thereby enhancing the efficiency of blockchain operations. For blockchain nodes on the aggregation main platform, there's a requirement to store and validate data related to the subject only. For the edge cluster, only need to manage and store the multiple blocks within this cluster chain, do not need to engage with other blocks at the edge of the cluster chain. The blockchain system of the cloud system stores and monitors the blockchain operation data and electric data of the entire grid, facilitating the improvement of the comprehensive power supply capacity of the entire grid based on trusted on-chain data.

B. Business Architecture

Built upon a cloud-native architecture, the Blockchain as a Service (BaaS) platform dynamically scales resources in response to the count of affiliated blockchains managed by the edge cluster.

The blockchain gateway functions as a universal connector for various applications, offering features such as protocol conversion, permission interception, data validation, and traffic regulation. Additionally, it provides a set of standard blockchain interfaces to external systems.

The blockchain console provides a comprehensive suite of visual on-chain governance functions, including but not limited to: network maintenance, node management, transaction handling, channel control, blockchain browsing, smart contract management, network topology visualization, and a pending approval system. By integrating a user permission module, the blockchain system enables role-based access control. Furthermore, it establishes secure management over on-chain certificates, smart contract execution, inter-node data transmission, and endorsement strategies. It also supports monitoring capabilities with alert functionalities. The business architecture diagram is shown in Fig. 2.

C. Technical Architecture

The BaaS system is integrated with the following technologies and platforms:

(1) JRESCloud development framework, SpringBoot + Dubbo;

(2) JRESConsole Microservice console;

(3) HUI2.0 development framework, VUE + micro-front-end architecture;

(4) HSIAR 1.2.32, technology gateway, analogy to Nginx;

(5) SEE2.0 integrated deployment/monitoring platform.

In addition, the operating system adopts CentOS7.6, Lense 6.0.80 and Galaxy Kirin V10, the data transmission protocols include HTTP(S), T2, T3 and gRPC, the development language uses Java8, Node10 and Go 1.14.4, and the database uses MySQL 5.7.28. The third-party components include Redis 4.0, Zookeeper 3.4.14, RabbitMQ 3.7.16, Longhorn 1.1.1, build/compile tools Maven 3, Webpack 4, GNU Make 4.2, and the container running environment is 18.04. The container orchestration tool is Kubernetes 1.18.8. For a visual representation of the system's technical architecture, please refer to Fig. 3.

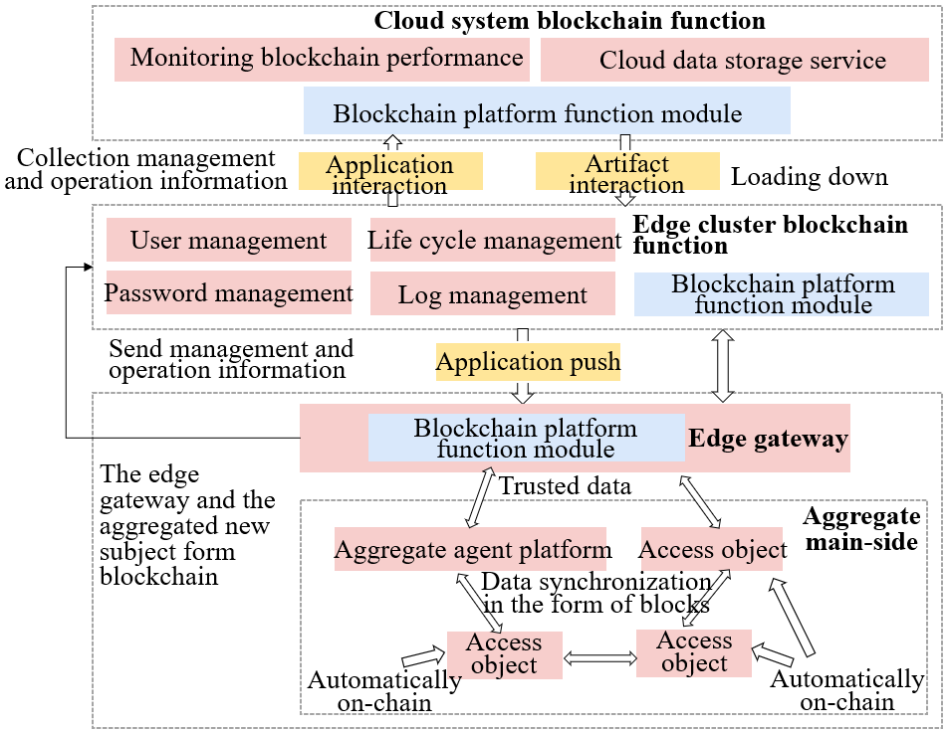

Fig. 1. The overall architecture of BaaS system

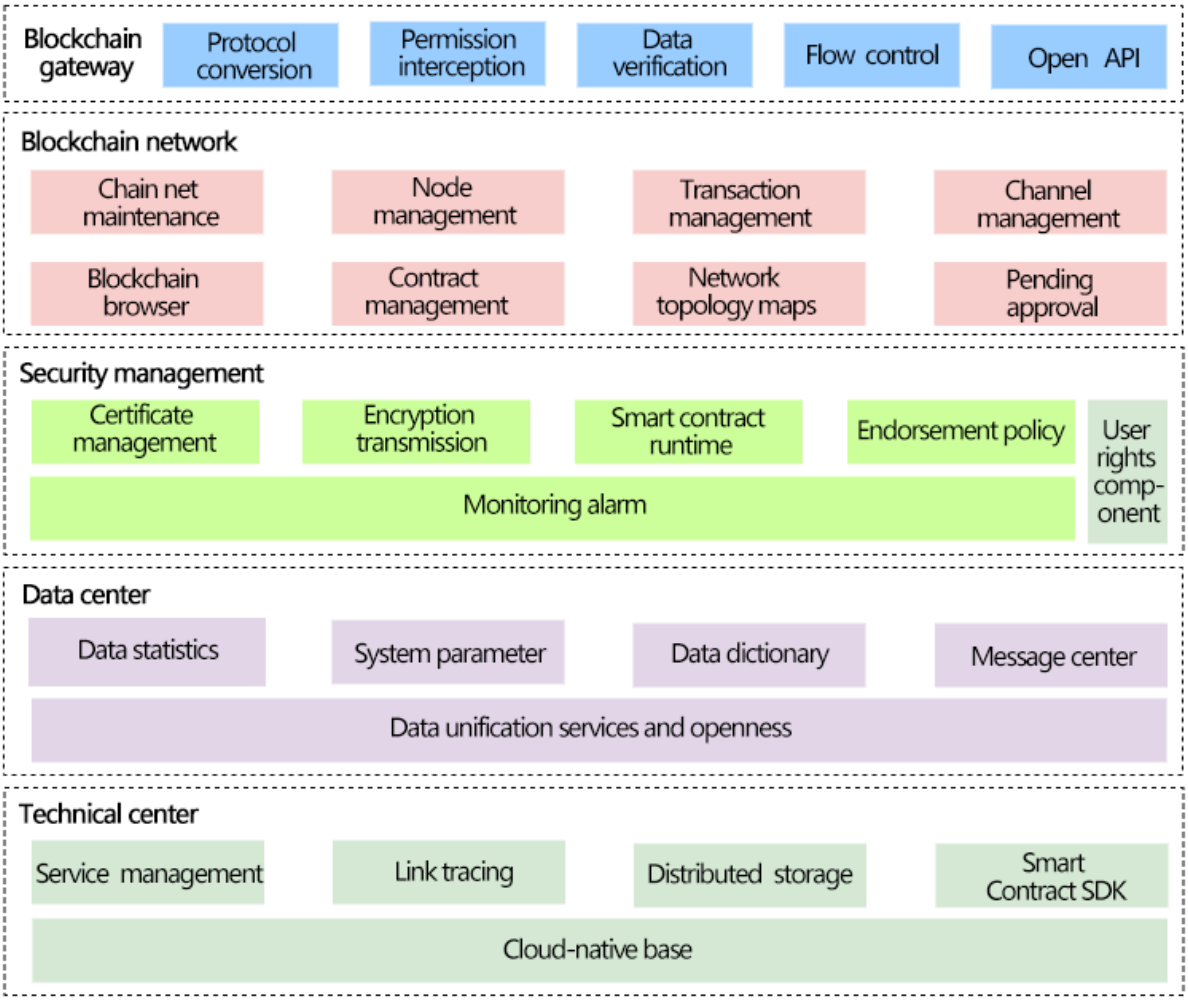

Fig. 2. The business architecture of BaaS system

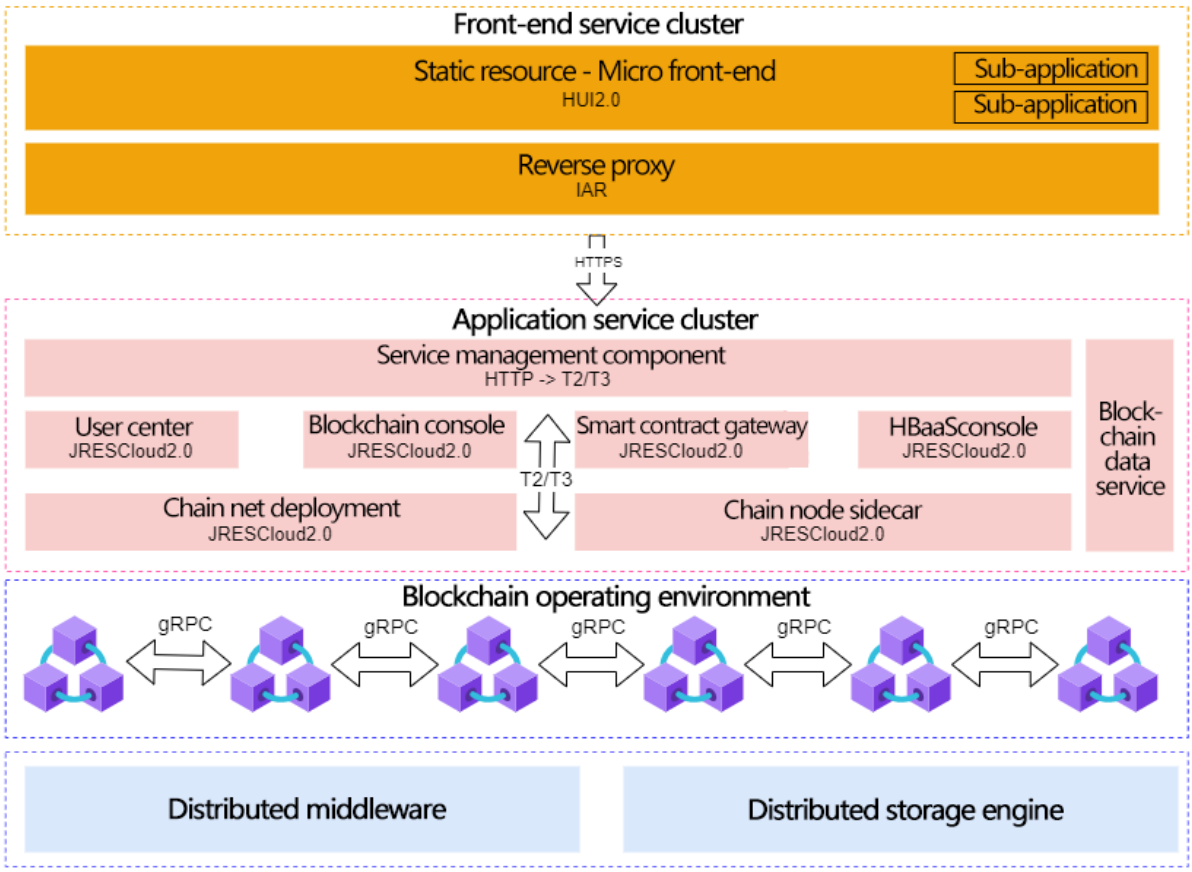

Fig. 3. The technical architecture of BaaS system

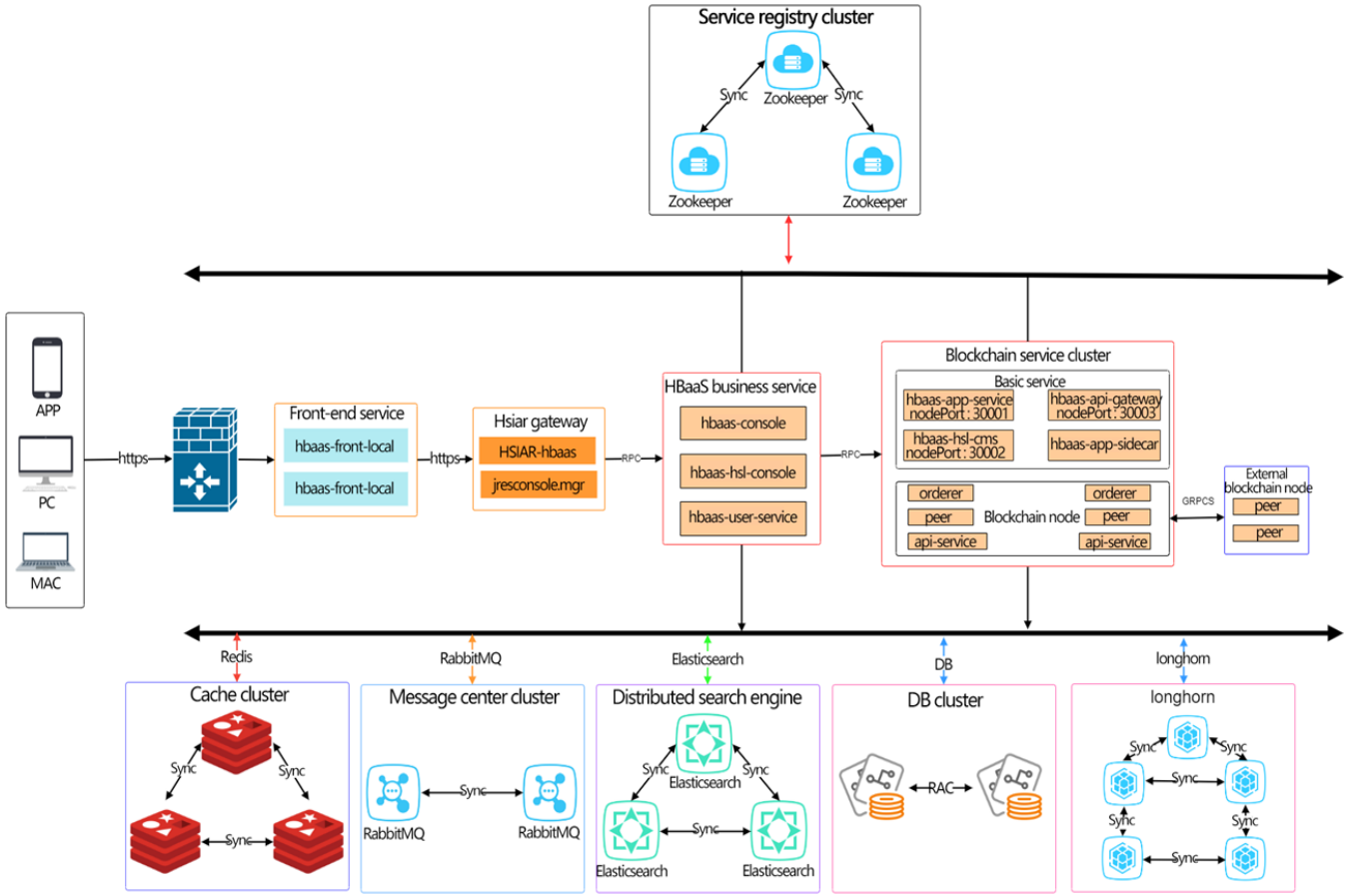

Fig. 4. Network topology maps

D. System Deployment Scheme

The system's development, implementation, deployment, operation, and maintenance processes all adhere to the requirements outlined in the Guidelines for the Technical Management and Control of Business Systems and Public Services on the Dispatching Cloud of China Southern Power Grid. The core of our approach is centered around the main node of the dispatching cloud, where we embrace "cloud-native" development and deployment practices. We make use of cloud-native components such as message buses, cloud service buses, and cloud platform resources encompassing computing, storage, network, and databases provided by the dispatching cloud. Furthermore, within this project, we have transformed the functional business processes of "collection, processing, storage, analysis, and display" into microservices within the cloud business platform layer. This transformation allows for a unified service scheduling system that operates seamlessly based on the scheduling cloud. It's worth noting that our system's deployment adheres to the principle of ensuring that service application functions are fully compatible with the scheduling cloud, ensuring optimal performance and functionality.

Fig. 4 illustrates the network topology structure of BaaS system. The blockchain system is deployed within the secure access zone, capable of receiving HTTPS requests from the external network. It access front-end static resources through the network switch, and the back-end interface is routed to the specified microservice through the hsiar gateway proxy. The blockchain systems rely on the following middleware components:

(1) Service registry based on zookeeper;
(2) Cache service based on Redis;
(3) Messaging components based on RabbitMQ;
(4) Search service based on ElasticSearch;
(5) Database storage services based on MySQL;
(6) Containerized distributed file storage based on Longhorn.

IV. Core Technologies

A. Trusted Data On-chain

Data on-chain refers to the practice of storing data in the blockchain to guarantee its immutability. The blockchain platform's function module is utilized to store critical data on the chain to prevent data from being illegally tampered with, and provide security protection for key information related to settlement for market players participating in cloud-edge integrated intelligent scheduling operation. The detailed technical architecture of data on-chain is shown in Fig. 5.

To facilitate on-chain data storage, it is necessary to establish a chain network on the edge cluster side, and join the chain network as a core role to control nodes and channels on the chain. Following this, the border gateway and aggregator deploy nodes separately and connect to the chain network to engage in the consensus process.

The data collected by the monitoring terminal needs to be batched and sent to the blockchain node located at the border gateway. It is then synchronized to other chain net nodes after a specific time interval. Within this chain network, which comprises three types of nodes—edge clusters, border gateways, and aggregators—an entity will issue a set of blockchain certificates. Typically, only one node is deployed,

but in cases where multiple nodes are deployed, they can only share the same set of certificates and have a single voting right. Any attempt by a node to tamper with the data will be ineffective.

In addition, this project has implemented various trusted measures to ensure the credibility of data on-chain. These secure and reliable measures guarantee the integrity of data stored on the blockchain.

(1) Trusted Data Source: In this project, electrical terminal equipment is directly connected to blockchain nodes for on-chain data submission, eliminating intermediary systems and data processing, this guarantees that the data no-chain is first-hand. In addition, each device is equipped with its own unique identifier and digital certificate. These devices submit data to the blockchain network with the corresponding unique identifier as their identity, which can facilitate the traceability of the data source.

(2) Trusted Network Communication: Secure and reliable TLS (Transport Layer Security) connections are established through TLS digital certificates and blockchain nodes. This guarantees the credibility and security of the network layer, preventing middleman attacks.

(3) Trusted Equipment: Maintenance and operation of equipment and blockchain nodes require controlled equipment access with corresponding access certificates for upgrades and maintenance. Unauthorized users are restricted from performing maintenance and modifications.

(4) Trusted Software System: The software system, such as blockchain nodes, undergo rigorous security testing before deployment to prevent security vulnerabilities and unauthorized data modifications.

(5) Trusted Smart Contract: Deployment and upgrades of smart contracts necessitate approval from alliance members and require consensus across the entire network, ensuring the trustworthiness of the smart contract.

B. Trusted Data Comparison

Trusted comparison refers to the monitoring terminal collecting data directly on-chain, serving as a trusted data source. Another data source obtains data from aggregators, which originates from aggregator platforms. By comparing and verifying data from multiple parties, trusted electric power data can be established. For a detailed view of the technical architecture of trusted comparison, please refer to Fig. 6.

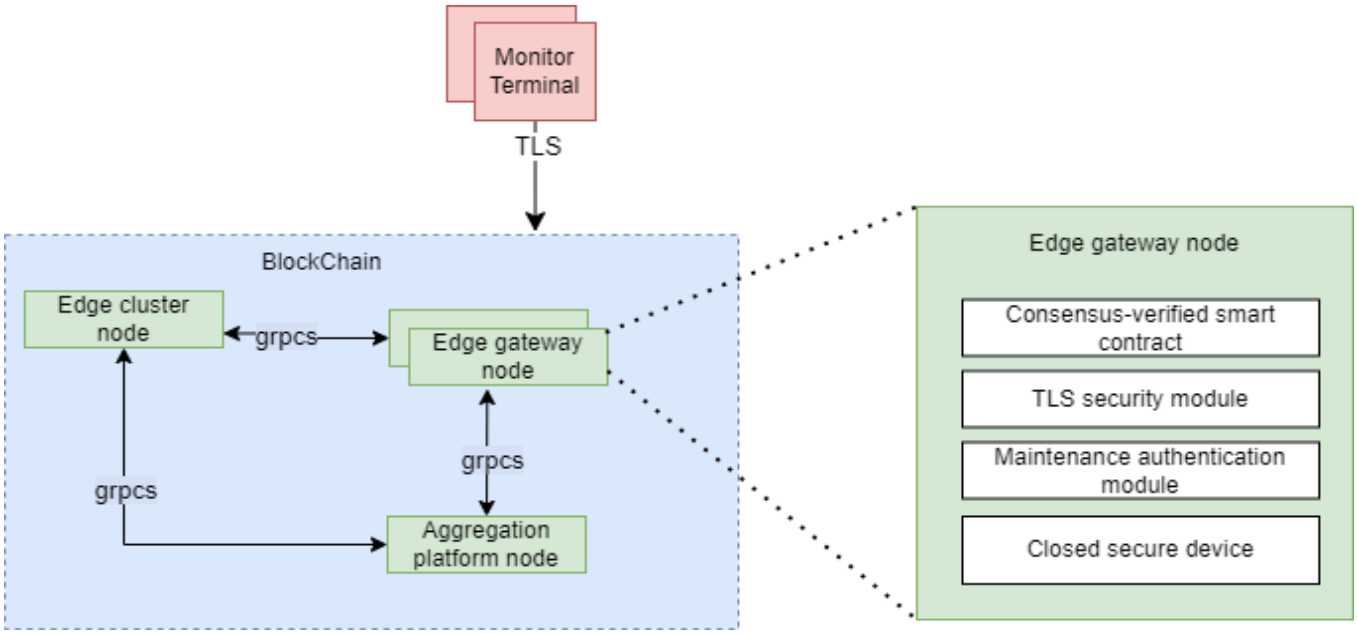

Fig. 5. The technical architecture of data on-chain

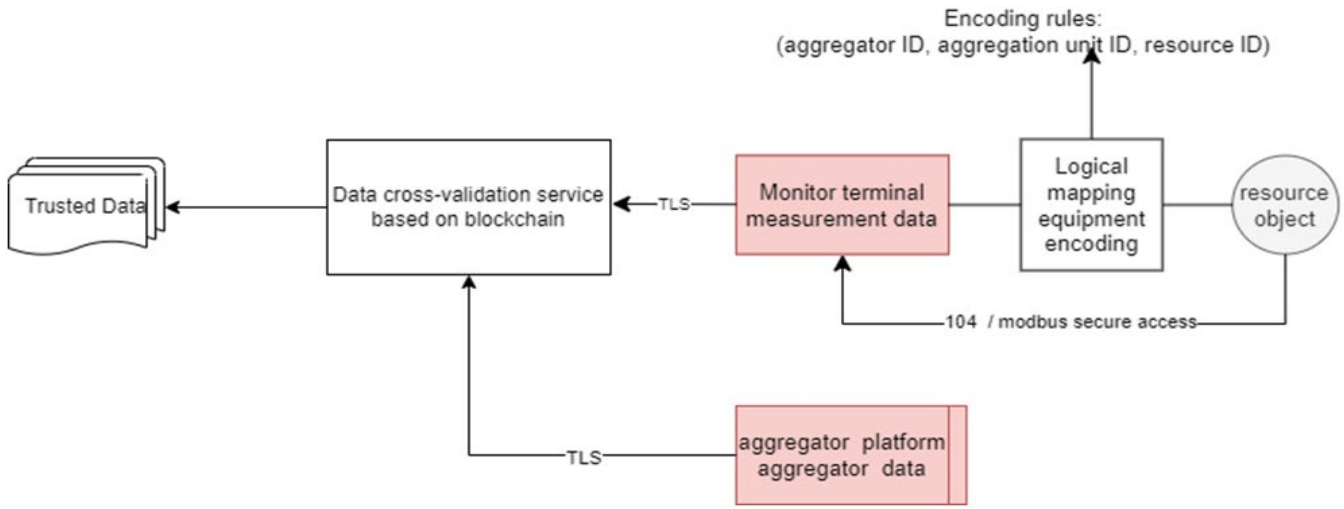

Fig. 6. The technical architecture of trusted comparison

There are two methods of trusted comparison:

(1) Intra-day Routine Comparison: Data comparison at a certain time interval (such as 1 hour);

(2) Daily Comparison: Data comparison between similar days (such as this Wednesday and last Wednesday).

There are three dimensions of trusted comparison:

(1) Comparison of the own data of data source: This dimension involves comparing data from within the same data source;

(2) Comparison of single data source itself: Here, data from a single source is compared internally;

(3) Comparison between different data sources: This dimension focuses on comparing data between different data sources, enabling cross-source validation.

We execute the comparison algorithm using various methods and dimensions, obtain the comparison results, and document the number of comparisons made.

It should be noted that intra-day routine comparison allows for large total errors and fluctuation errors, such as ±10%, within a short period of time. On the other hand, daily comparison mainly controls the overall error, and it is necessary to prevent the gradual increase of the total amount, which resulting in too large a fluctuation range. To achieve this, stricter limits are imposed on the overall total amount and the fluctuation error range, often set at around ±5%. Data that falls within this error range, as compared and validated, can be considered as trustworthy power data.

C. *Edge Cluster Data Transmission*

In order to present the chain net data and on-chain data of edge clusters, which are deployed within the secure access zone, on the cloud page, the collected data needs to be ferried from the secure access zone to the security zone II. The ferry mode is file synchronization, and the file format must comply with the E language specification.

There are two types of data that require synchronization:

(1) Metadata Information: This includes fundamental details about the Chain, Channel, and Node;

(2) On-chain Data: This includes fundamental details about the Block data and Transaction.

As illustrated in Fig. 6, for metadata information, data can be directly retrieved from the hsl-console database. For on-chain data, the API Server service itself listens for blockchain events, supports event processing extensions, and writes block and transaction information obtained to a message queue (MQ). The data acquisition module then listens for message consumption. The data collection production end through the above two data sources, writes the corresponding file conforming to the E language standard according to the data type, and stores it in the synchronization directory specified by the edge cluster. Then the file is synchronized from the secure access zone to the corresponding directory in the security zone II. The data collection and consumption end deployed in the security zone II can obtain the corresponding file and extract the synchronization data from it. This data source can then be utilized for subsequent cloud-based presentations.

The edge cluster data transmission is also trusted. Through end-to-end encryption, both the edge and the cloud employ the other party's public key for encryption. This ensures that the other side can decrypt because of the private key, and any intermediate node cannot decrypt, view or tamper with. The technical architecture of edge cluster data transmission is shown in Fig. 7.

D. *Optimized Transaction Authentication*

Given the diverse constraints imposed by varying environmental resources, it is necessary to consider the transmission of on-chain data in a low bandwidth network environment.

Our analysis reveals that every transaction sent to the blockchain necessitates the use of a digital signature for transaction authentication. However, it's important to note that the digital signature data is appended to the transaction, resulting in an increase in transaction size. This, in turn, consumes more network bandwidth and storage space.

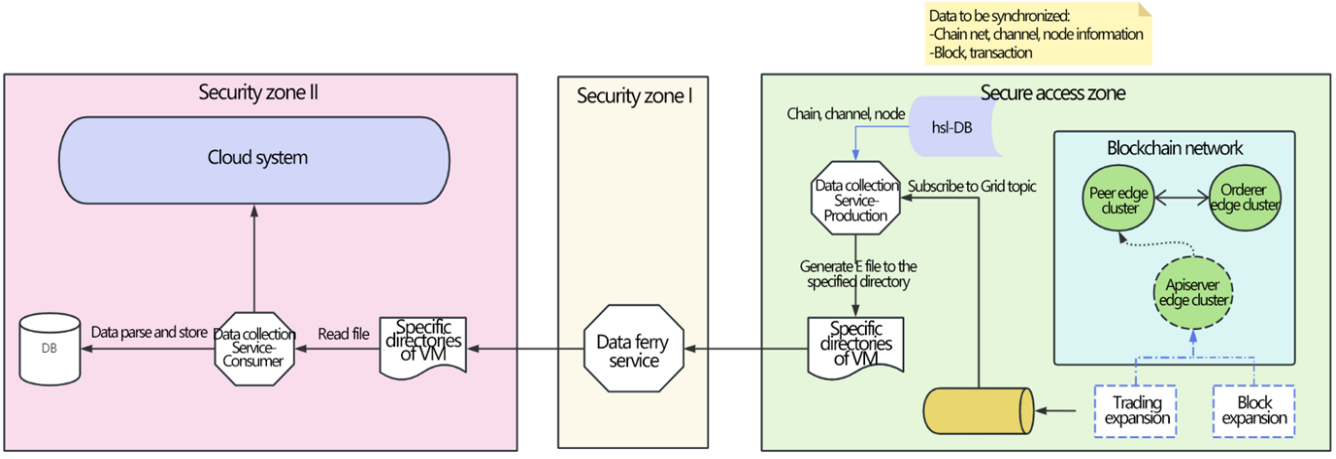

Fig. 7. The technical architecture of edge cluster data transmission

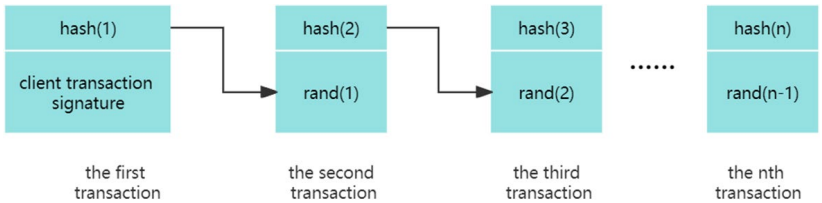

Fig. 8. Authenticating transactions through combined digital signature and hash verification

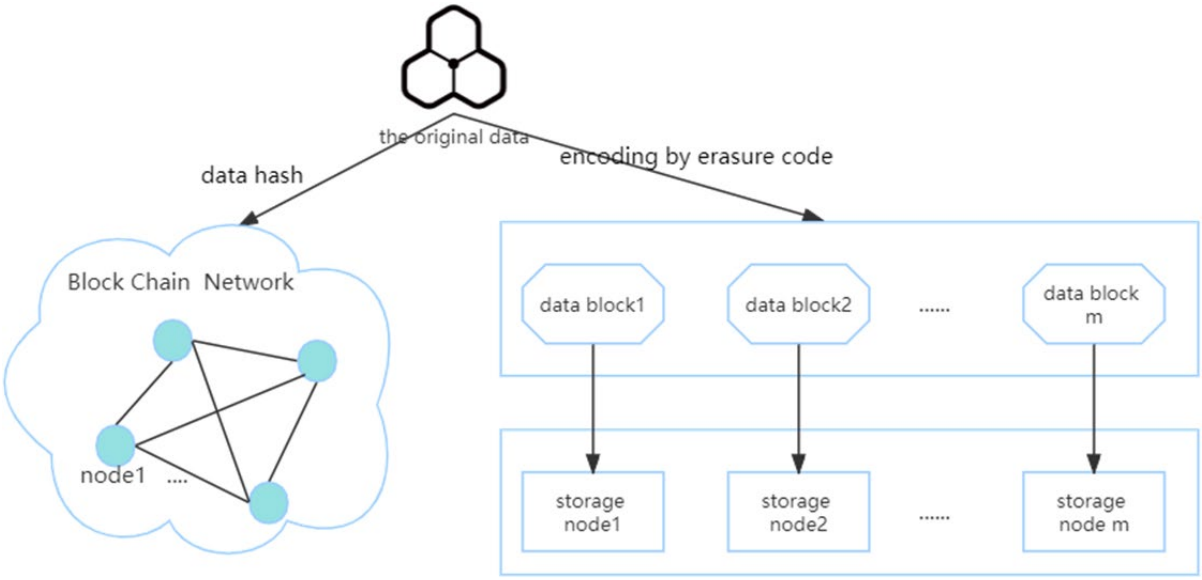

Fig. 9. Procedure of light weight storage

On the secure communication channel, the respective devices establish direct connections with blockchain nodes. For two-phase or three-phase commit blockchain systems like Fabric, where multiple blockchain nodes have endorsed and signed transactions, the client, which is the device, also verifies the endorsed and signed transactions. As a result, the client can streamline the transaction process by eliminating the need for a digital signature with each transaction. Instead, during the second phase of the commit, a chain of hash validations can be employed. The process of authenticating transactions through a combination of digital signatures and hash verification is illustrated in Fig. 8.

Here are the details of the process:

(1) The device prepares to initiate an on-chain request by generating a random number, rand1. It then hashes rand1 to obtain hash1 and creates a unique transaction string identifier identifier1.

(2) The device submits a transaction request with digital signature to the node. This request includes the previously calculated hash1 and identifier1.

(3) The blockchain system verifies the user's digital signature. If the verification is successful, the system performs with transaction processing and stores both hash1 and identifier1 on the blockchain;

(4) In the second transaction, different from the digital signature operation on the transaction, the device provides the original hash1, namely rand1, as one of the bases for the blockchain node to authenticate the new transaction, and no digital signature is performed. Additionally, the device can supply HASH2 and identifier1 as supplementary information. HASH2 is generated by creating a new random number, rand2, and hashing it. The client retains rand2 for subsequent transactions.

(5) Upon receiving a formal transaction from the user, blockchain nodes follow different procedures depending on whether the transaction is digitally signed or not. For digitally signed transactions, existing technology certification is applied. For transactions without digital signatures, the authentication process is as follows:

a) Query hash1 in the ledger and rand1 in the current transaction according to identifier1;

b) Calculate the hash function (rand1) and compare the result with the hash1 from the previous transaction;

c) If the calculated hash value and hash1 match, it indicates successful authentication, and the transaction is deemed legal. This is because the irreversible nature of the hash algorithm ensures that rand1 was derived from hash1.

To mitigate the risk of malicious users dedicating substantial resources to crack the hash algorithm, it's advisable to opt for a highly secure hash algorithm like SHA256. Additionally, you can impose a time limit on the validity of rand1. For instance, even if the provided rand1 is accurate, if the time exceeds 10 minutes, the authentication should fail, and the original digital signature logic must be reverified. This approach adds an extra layer of security to the authentication process.

E. Light weight Storage Nodes

Due to the constraints imposed by various environmental resources, it becomes essential to contemplate the operation of blockchain nodes on devices with limited storage capacity. For instance, edge gateways and certain partial aggregation subject platforms require the design of lightweight node solutions to ensure efficient operation.

Lightweight nodes eliminate the need to store the entire blockchain ledger, effectively reducing the demands on storage resources. Instead, they store data hashes, which serve to verify both data integrity and whether any tampering has occurred. If resources permit, lightweight nodes may also opt to store partial data shards. These data blocks represent block data that must be stored and encoded into the corresponding number of data fragments using erasure coding, as depicted in Fig. 9. This approach enables efficient storage management while maintaining data security.

Taking into account the presence of potentially malicious nodes, the data sharding algorithm is designed as follows: let the total number of data shards after erasure code coding be equal to the number of blockchain nodes, and the number of check blocks be equal to the fault tolerance coefficient of the blockchain consensus algorithm multiplied by the total number of data shards. This design helps enhance the security and fault tolerance of the blockchain network in the face of potential malicious nodes.

Table I: Comparison of traditional system and proposed system

Comparison Item	Traditional System	Proposed System
Architecture	Single blockchain structure	Cloud-Edge Collaborative Multi-Chain
Scalability	Difficult to scale	Horizontally scalable
Cloud Resource Consumption	Huge consumption	Reduced consumption, offload computing to edge clusters
Blockchain Storage Resource	Replicated storage, high resource consumption	Erasure coding, reduced redundancy, lower resource consumption
Blockchain Network Resource	Larger packets. Signature data in every client request	Smaller packets. Hashes instead of signatures for some requests
Blockchain Computing Resource	High signature verification consumption	Lower hashing consumption
Online User Support	Limited, varies for different systems	theoretically unlimited
Data Credibility	Hard to ensure	Greatly improved

There are various blockchain consensus algorithms available, each with its own fault tolerance characteristics. For instance, the PBFT algorithm supports 1/3 fault tolerance, meaning that the failure or malignancy of up to 1/3 of the nodes in the entire system will not disrupt the normal operation of the blockchain. Meanwhile, the RAFT algorithm supports 1/2 fault tolerance, allowing the failure or malignancy of up to 1/2 of the nodes in the system without affecting the blockchain's normal operation. As an example, consider a scenario with 4 blockchain nodes and the use of the PBFT consensus algorithm. In this case, the number of verification blocks would be 1, calculated as (4-1)*(1/3), while the corresponding data blocks would be 3. Consequently, the encoded data can tolerate the unavailability of 1/3 of the data shards, aligning with the fault tolerance characteristics of the PBFT blockchain consensus algorithm.

V. Comparison of Solutions

By leveraging the hierarchical multi-chain architecture design, cloud-edge collaboration, and technical solutions such as Lightweight Storage Nodes and optimized transaction authentication, the system's capabilities compared to traditional solutions are outlined in Table I. This comparison demonstrates its superior ability to cater to the extensive data on-chaining requirements within the electric power industry.

Scalability stands out as a pivotal advantage of the proposed system when compared to traditional counterparts. As new subordinate aggregators acess the edge clusters, the system can dynamically request fresh blockchain resources from BaaS to establish and integrate into new blockchain channels. Conversely, when aggregators exit, BaaS can also dynamically reclaim resources. Based on the scalability features, the proposed system allows for the addition of new blockchains through horizontal scaling. In theory, there exists no upper constraint on the number of aggregators and power data that can be incorporated into the blockchain. The traditional single blockchain structure will encounter bottlenecks in the face of increasingly complex and huge data requirements, while the hierarchical multi-chain architecture provides more space and resources for the system to meet the growing challenges in the future. The advantage of this architecture is that new chains can be added dynamically according to demand, thus effectively sharing the load and ensuring the stability and sustainability of the system.

Another pivotal advantage of the proposed system is its reduced resource requirements. Through the hierarchical multi-chain architecture, the performance demands placed on the cloud platform and individual blockchains are substantially diminished. This enhanced efficiency better supports the widespread integration of distributed energy nodes and facilitates efficient and dependable data sharing.

The introduction of lightweight storage node solutions can further curtail the storage resource demands of individual blockchain nodes. A comparison between lightweight node storage and replicated storage is illustrated in Fig. 10. The analysis reveals that the proposed solution can reduce storage resource requirements by several times or more in contrast to traditional solutions.

By employing optimized transaction authentication, there are scenarios where digital signatures can be substituted with hash verifications, resulting in reduced resource consumption. This optimization scheme allows the system to adapt to various transaction and verification requirements more flexibly, and can help to save computing and network resources to a certain extent. It not only improves the efficiency of the system, but also reduces the operation cost, and provides stronger support for the sustainable development and scalability of the system.

Data credibility represents another vital distinguishing feature. Various methods are employed to guarantee data credibility before it is placed on the blockchain. The blockchain data service conducts multi-party data verification and comparison, culminating in the production of trusted power data. This emphasis on data integrity and authenticity sets the system apart.

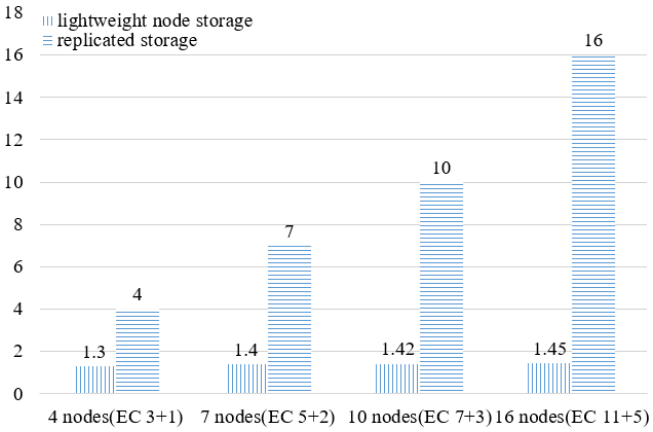

Fig. 10. Comparison between lightweight node storage and replicated storage (PBFT)

VI. Conclusion

Addressing the demands of the digital transformation of China Southern Power Grid, this paper puts forward a BaaS system based on intelligent scheduling and cloud-edge operation platform. It delves into the challenges arising from

the exponential increase in information data and the intricacies of credibility verification due to the extensive participation of market stakeholders in the power market system. In response to these challenges, a set of core technical solutions has been proposed. These include a two-level multi-chain architecture of cloud-edge collaboration, trusted data on-chain, trusted data comparison, edge cluster data transmission, optimized transaction authentication, and lightweight storage nodes.

The system successfully achieves trusted on-chain operations for aggregated subject data and ensures the comparison and verification of data trust. It effectively resolves issues related to the normal operation of the blockchain network in low-resource environments. Additionally, it enables the management of the blockchain by the edge cluster, encompassing its subordinate aggregation main platform and edge gateway. Moreover, the system furnishes trusted data support for the cloud system to monitor the operation of the entire blockchain network and facilitates intelligent power market dispatching.

REFERENCES

[1] Y. Xu, J. Hu, and H. Zhou, "Blockchain-based trading and settlement framework for electricity markets," in *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, Beijing, China, 2021, pp. 243-246. https://doi.org/10.1109/CISCE52179.2021.9445983

[2] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: a methodology perspective," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 353-385, 2023. https://doi.org/10.1109/COMST.2022.3204702

[3] S.C. Cha, C.L. Chang, Y. Xiang, T.J. Huang, and K.H. Yeh, "Enhancing OAuth with blockchain technologies for data portability," in *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 349-366 2023. https://doi.org/10.1109/TCC.2021.3094846

[4] J. Witt and M. Schoop, "Blockchain technology in e-business value chains," *Electronic Markets*, vol. 33, pp. 15, 2023. https://doi.org/10.1007/s12525-023-00636-5

[5] A. Mishra and P. Jena, "Application of blockchain technology for microgrid restoration," *IEEE Transactions on Power Delivery*, vol. 38, no. 3, pp. 1810-1825, 2023. https://doi.org/10.1109/TPWRD.2022.3226659

[6] B.V.S. Babu and K.S. Babu, "The purview of blockchain appositeness in computing paradigms: A survey," *Ingénierie des Systèmes d'Information*, vol. 26, no. 1, pp. 33-46, 2021. https://doi.org/10.18280/isi.260104

[7] Feroz Khan, A.B, "ECO-LEACH: A Blockchain-Based Distributed Routing Protocol for Energy-Efficient Wireless Sensor Networks," *Information Dynamics and Applications*, vol. 2, no. 1, pp. 1-7, 2023. https://doi.org/10.56578/ida020101

[8] V.L. Narayana, and D. Midhunchakkaravarthy, "A trust based efficient blockchain linked routing method for improving security in mobile ad hoc networks," *International Journal of Safety and Security Engineering*, vol. 10, no. 4, pp. 509-516, 2020. https://doi.org/10.18280/ijsse.100410

[9] J. Zhang, C. Bao, M. Xu, Y. Jin, C. Zhou, and J. Xie, "Distribution network distributed resources application framework and key technologies based on cloud-edge-device collaboration," in *2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2)*, Chengdu, China, 2022, pp. 1888-1892. https://doi.org/10.1109/EI256261.2022.10116961

[10] Q. Zheng, L., Wang, J. He, and T. Li, "KNN-based consensus algorithm for better service level agreement in blockchain as a service (BaaS) systems," *Electronics*, vol. 12, no. 6, p. 1429, 2023. https://doi.org/10.3390/electronics12061429

[11] K. Wang, Z. Tu, and Z. Ji, "PoTA: A hybrid consensus protocol to avoid miners' collusion for BaaS platform," *Peer-to-Peer Networking and Applications*, vol. 15, no. 4, pp. 2037-2056, 2022. https://doi.org/10.1007/s12083-022-01337-0

[12] R. Rahmadewi, R. Hanifi, T.N. Padilah, R. Amalia, R. Sya'bani, and A. Maulana, "HE-Cool V1.0: Control model of hybrid evaporative cooler prototype," *Journal Européen des Systèmes Automatisés*, vol. 55, no. 1, pp. 89-96, 2022. https://doi.org/10.18280/jesa.550110

[13] M. Chen, Z. Shen, L. Wang, and G. Zhang, "Intelligent energy scheduling in renewable integrated microgrid with bidirectional electricity-to-hydrogen conversion," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2212-2223, 2022. https://doi.org/10.1109/TNSE.2022.3158988

[14] Z. Yin, F. Xu, Y. Li, C. Fan, F. Zhang, G. Han, and Y. Bi, "A multi-objective task scheduling strategy for intelligent production line based on cloud-fog computing," *Sensors*, vol. 22, no. 4, p. 1555, 2022. https://doi.org/10.3390/s22041555

[15] K. Yuan, Y. Yan, L. Shen, Q. Tang, and C. Jia, "Blockchain security research progress and hotspots," *IAENG International Journal of Computer Science*, vol. 49, no. 2, pp. 433-444, 2022.

[16] N. A. M. Razali, W. N. Wan Muhamad, K. K. Ishak, N. J. A. M. Saad, M. Wook, and S. Ramli, "Secure blockchain-based data-sharing model and adoption among intelligence communities," *IAENG International Journal of Computer Science*, vol. 48, no. 1, pp. 18-31, 2021.

[17] R. Vatambeti and V. K. Damera, "Gait Based Person Identification Using Deep Learning Model of Generative Adversarial Network (GAN)," *Acadlore Transactions on AI and Machine Learning*, vol. 1, no. 2, pp. 90-100, 2022. https://doi.org/10.56578/ataiml010203

[18] N. S. Divya and R. Vatambet, "Detecting False Data Injection Attacks in Industrial Internet of Things Using an Optimized Bidirectional Gated Recurrent Unit-Swarm Optimization Algorithm Model," *Acadlore Transactions on AI and Machine Learning*, vol. 2, no. 2, pp. 75-83, 2023. https://doi.org/10.56578/ataiml020203

[19] P. M. B. Muddumadappa, S. D. K. Anjanappa, and M. Srikantaswamy, "An Efficient Reconfigurable Cryptographic Model for Dynamic and Secure Unstructured Data Sharing in Multi-Cloud Storage Server," *Journal of Intelligent Systems and Control*, vol. 1, no. 1, pp. 68-78, 2022. https://doi.org/10.56578/jisc010107

[20] A. Nhlabatsi, K.M. Khan, J.B. Hong, D.S. Kim, R. Fernandez, and N. Fetais, "Quantifying satisfaction of security requirements of cloud software systems," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 426-444, 2023. https://doi.org/10.1109/TCC.2021.3097770

[21] T. Yeh and C. Sun, "Enhancing the reliability of cloud data through identifying data inconsistency between cloud systems," *Information Systems Frontiers*. https://doi.org/10.1007/s10796-023-10405-6

[22] J. Youn and Y.H. Han, "Intelligent task dispatching and scheduling using a Deep Q-Network in a cluster edge computing system," *Sensors*, vol. 22, no. 11, p. 4098, 2022. https://doi.org/10.3390/s22114098

[23] S. Xu, Y. Qian, and R. Q. Hu, "Edge intelligence assisted gateway defense in cyber security," *IEEE Network*, vol. 34, no. 4, pp. 14-19, 2020. https://doi.org/10.1109/MNET.011.1900407

[24] R. Gao, Q. Li, L. Dai, Y. Zhan, and Y. Xia, "Workflow-based fast data-driven predictive control with disturbance observer in cloud-edge collaborative architecture," *IEEE Transactions on Automation Science and Engineering*. https://doi.org/10.1109/TASE.2023.3270203