Research on Blockchain-Based Power Data Storage Scheme

Peiguang Chen[1], Zihao Tian[1], Dong Wang[1], Yeyang Zhu[2,*]

[1] State Grid Economic And Technical Research Institute Of Jilin Electric Power., LTD
[2] University of Southern California

Abstract. Blockchain technology was invented for bitcoin. It serves as a new computing paradigm with a decentralized framework. For its characteristics such as decentralization, tamper-proofing, and traceability, this technology has been widely used in various industry sectors. Currently, the power industry, as China's basic energy industry, is closely linked to national economic development. In the power industry, power data storage and dispatching are of paramount importance. However, there are some security problems with traditional storage methods. Given this, this paper proposed a blockchain-based power data storage scheme, to enhance the security of power data storage.

1 PREFACE

The construction and improvement of smart grid infrastructure, especially the application of smart meters in substations, has become an important source of smart grid data. At present, as part of the basic national data, circuit data is associated with the stability and development of a country. Nowadays, the power data has permeated into macroeconomic, social life, and other aspects. It not only contributes to economic development but also enables cross-professional and cross-unit integration, thus improving the economic efficiency of enterprises. In the whole process, the smart grid data has become more and more important so that scholars also began to focus on studying circuit data storage security. There are various data risk factors in the existing power system. For example, attackers may attack, intentionally modify, or delete the circuit data stored in the cloud. At present, the power data is stored in a centralized way. It means when the data storage platform collapses, a large amount of data will be lost. For this reason, it is necessary to discuss the current power data storage problems. Meanwhile, for the improvement of technology, as one of the emerging technologies, blockchain has the characteristics of decentralization and tamper-proofing, which can make up for the defects in power data storage nowadays.

2 INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

2.1 P2P Network

P2P is a way of structuring distributed applications such that tasks can be distributed in each node without the need of a central server. The current central network architecture is C/S, where a central server is required. When the client issues a request, the server will reply directly in response to the request. In the P2P network, each node across the network boundaries can send and receive data. In this way, each node can not only act as the client but also receive services provided by other nodes. At present, P2P network has the characteristics of decentralization, privacy protection, and scalability in the application of blockchain technology. In the application process, the required resource information is distributed at blockchain network nodes, and the transaction process is carried out at each node without the need of third-party access. Blockchain provides different levels of anonymity and adopts a broadcasting mechanism for the transmission of node information to ensure privacy protection. [1]

2.2 Cryptography

As one of the key elements of blockchain technology, cryptography plays a basic role in the realization and improvement of blockchain technology and security protection. The development of blockchain and cryptography go hand in hand. The common cryptographic techniques in blockchain are the hashing algorithm, asymmetric encryption, and digital signature.

2.2.1 Hashing algorithm

Hashing algorithm can map binary plaintext strings of arbitrary size into shorter ones. Different hash values shall be obtained under different plaintext strings. Excellent hashing algorithms usually are highly efficient and difficult to reverse. Also, the hashing algorithms can be further divided into MD5 algorithm and SHA algorithm. The former is a widely used cryptographic hash function that results in a 128-bit hash value. The latter is an improved version of MD4 with higher

* Corresponding author: yeyangzh@usc.edu

security performance, but MD5 is proven to be not highly collision-resistant at present. SHA is not an algorithm but a family of hash functions. SHA-1 is the same as MD4 in terms of design principle and does not have the features of anti-analysis and anti-difference. Currently, to improve operational security, the SHA-2 algorithm is designed. The SHA-2 algorithm complements SHA-1 in terms of high collision-resistance.

2.2.2 Asymmetric Encryption

Asymmetric encryption can be considered as a major invention in the field of cryptography research. It can solve the problem of distributing keys in advance. In the asymmetric algorithm, the key can be subdivided into encryption key and decryption key. The encryption key, also known as the public key, is public and visible to others. The decryption key, also known as the private key, is generated by using a random algorithm and is private and kept secret from others. The asymmetric encryption algorithms commonly used nowadays include ElGamal, RSA, SM2, and elliptic curve algorithms, of which RSA is the most classic public key algorithm. The asymmetric encryption algorithms are more commonly used for permission verification in blockchains, such as data encryption and digital signature, which can improve the security and privacy of information stored on the blockchain.[2]

2.2.3 Digital Signature

Digital signature, also known as public key digital signature, is a scheme for verifying the identity of a sender based on the digital string sent by the sender, and the digital string cannot be forged. The digital signature is based on asymmetric encryption algorithms and is used to verify the integrity and source of the message. Its main algorithms include DSA and ECSDA. Also, the signature algorithm is often used in places with high-security requirements. Considering this, more signatures are created such as blind signatures, ring signatures, and group signatures. In addition, digital signatures have characteristics of irreversibility and availability. The former indicates that the private key cannot be forged by others, while the latter shows that a message which has encrypted using the private key can be decrypted using the public key, and the correctness and integrity of the message can be ensured.

2.3 Hyperledger

Hyperledger is the first open-source distributed ledger platform for enterprise application scenarios led by IBM. Unlike Bitcoin and Ethereum public blockchains, Hyperledger is a type of alliance chain. The joining of blockchain nodes requires identity authorization. The setting of the access mechanism greatly improves the consensus efficiency of transactions, which builds the foundation for future high-efficient business networks based on blockchain. In the smart grid, the data transaction in the store is more frequent, and the transaction amount involved is also relatively small. In this case, mining and paying miner fees will become a burden. Therefore, in this paper, we use Fabric as the blockchain architecture model to provide a better data transaction method for power data transactions.

3 POWER DATA STORAGE SCHEMES

3.1 Traditional Power Data Storage Method

With the emergence of new power grid infrastructures such as smart substations and smart meters, substation inspection robots collect power data as a replacement for staff. At present, substation inspection robots need to collect data from substation smart meters and transmit meter dashboard data to substation monitoring backstage in real-time through a wireless communication system. Then the data shall be processed through image parsing methods. After that, the power data shall be transmitted to the power data center through a dedicated power transmission device, to further realize the coordination between the electricity regulatory department and power supply company in remote and centralized control and management. In the power system, the inspection robots will collect a large amount of image data, and the image data will be parsed into power data and then transmitted to the power dispatch, so as to improve data security and timeliness. The current traditional power data storage method is mainly centralized storage and unified dispatching through the third-party power centralized control center. As shown in the figure, currently only substations and power data centers can be integrated and connected through a dedicated power network. It can not only meet the remote dispatching requirements of the power supply bureau but also achieve automated data collection through robots, so as to provide convenience for data storage.

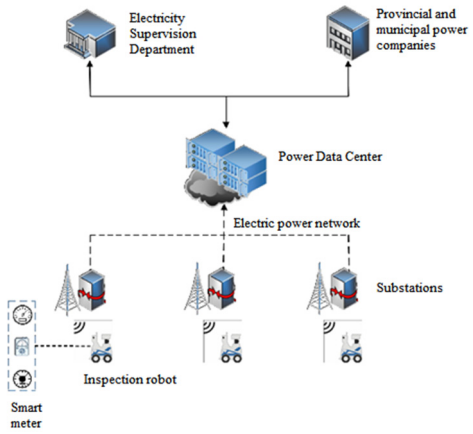

Fig 1. Traditional Power Data Storage Method

In the above power data storage method, the security problem is not solved. It is because the malicious monitoring and theft of power data may occur in the data generation and storage process, and some users even take the risk of data tampering. The traditional data

collection and control center will be affected by natural disasters. Compared to the existing storage methods, the traditional storage methods have security and high-cost problems.[3]

3.2 Blockchain-Based Power Data Storage Method

With the increase of power grid business data, the centralized storage method cannot meet the requirements for circuit data security and scalability. To find a better storage method, this paper proposed an opportunity blockchain storage method. As shown in the figure, the collection of power data is performed by inspection robots. After the smart meter reading, the image data transmitted by the smart meters is sent to the substation cloud server to achieve data reading. After the parallel vision is used to parse the meter image, the smart meter image in the cloud can identify the store data and transmit it to different substation nodes through the power transmission channel. The blockchain composed by substations can ensure the authenticity of power data and provide effective security storage and dispatching of power data.

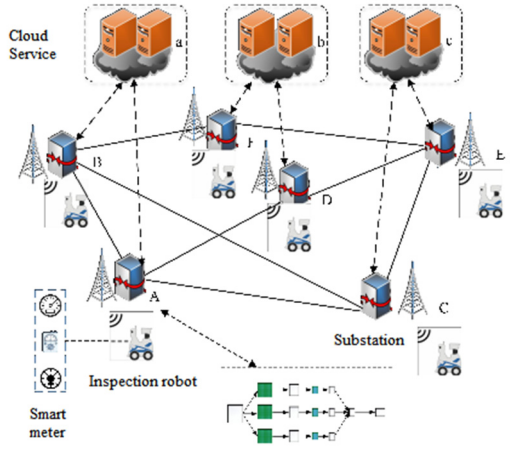

Fig 2. Blockchain-Based Power Data Storage Method

In the blockchain, decentralization, tamper-proof and other methods have achieved data security storage. The nodes in the blockchain can spontaneously maintain the data information at the nodes through consensus mechanisms and algorithms, and the data information and version information of different nodes are highly consistent.

4 POWER DATA STORAGE SCHEME DESIGN

4.1 Power Data Storage Scheme Requirements

The scheme design in this paper is based on the traditional circuit data storage methods. Blockchain technology is used to enhance the security and privacy of power data storage. In this paper, four roles are involved, namely, inspection robot, substation, substation personnel, and power company, all of which have their important responsibilities. For example, the inspection robot is responsible for collecting various meter data of substations. The substation personnel are responsible for standardizing the power data and initiating power transaction requests. The substation mainly acts as a blockchain node for the maintenance of the blockchain ledger. The last power company is mainly responsible for managing the blockchain nodes, including checking the information of organizational nodes, specifying the sorting nodes, and changing the organizational structure. Based on the analysis of the roles in the blockchain storage process, a functional requirement structure diagram is specially designed.

Table 1. Power Data Security Storage Requirements

Electricity data requirements	Electricity data storage
	Power data dispatch
	Power data query
	Power transaction inquiry
Blockchain management	Node management function
	Area management function
	User management function
	Contract management function

The purpose of the design in this paper is to enhance the security of power data storage by using a blockchain-based method. Given this, the blockchain functional requirements include four parts, namely node management, regional management, user management, and contract management. The requirements of the power scenario involve power data transactions, where the purpose of transactions is to change the state of the blockchain ledger. As an important part of the blockchain, the transactions should meet the storage and dispatching requirements of power data.[4]

Each power data transaction process shall be carried out according to the flow shown in the figure. For the power data request generated by the substation node, the substation manager will use the private key to digitally sign the transaction. After the transaction is generated, the transaction content will be transmitted across the whole network. The node will store the unverified transaction Hash value in the block, and then use the consensus algorithm to compete for the bookkeeping right and broadcast the bookkeeping result to the whole network. Then the node will be verified. When the node passes the verification, the power data can be entered into the blockchain. After the power data transaction gets completed successfully, the power data transaction content on the blockchain can be queried, which includes two parts, that is, power data query and power transaction query.

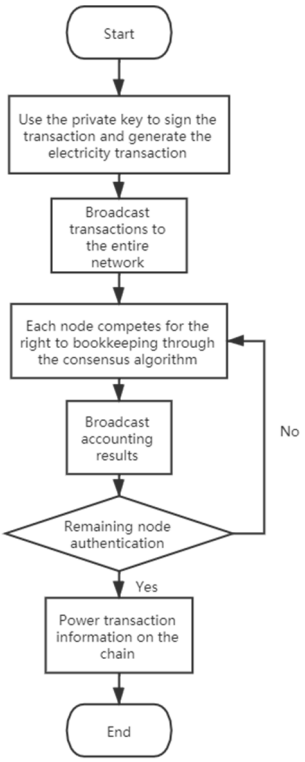

Fig. 3 Power Data Transaction Process

Except for the above functions, the power data security storage scheme also needs to consider the requirements of confidentiality, security, and timeliness.

4.2 Power Data Information Scheme Design

4.2.1 Blockchain System Architecture

The modular design is implemented according to the Hyperledger architecture. By combining the power data transaction and blockchain construction design, this paper finally determines the architecture of the power blockchain as shown in the figure.

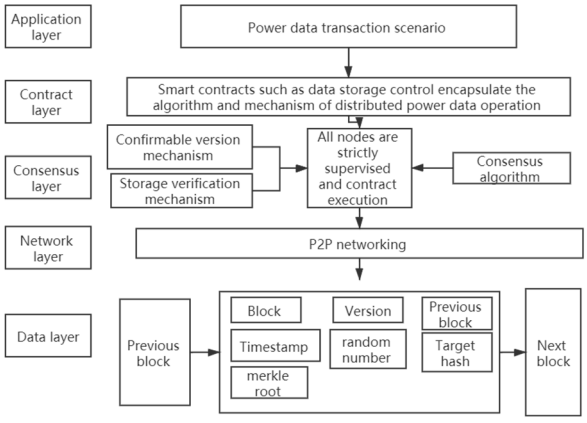

Fig. 4 Layered Structure of Power Blockchain

In this paper, the power blockchain architecture is divided into five layers in the order of top to bottom, which are application layer, contract layer, consensus layer, network layer, and data layer.

(1) Application Layer

The application layer is mainly designed to encapsulate the blockchain network transaction scenarios and application cases, which includes power data storage and power data dispatching. In power data storage, blocks produced through hash functions are used, and asymmetric cryptographic algorithms are used to enhance security. In the decentralized system, credit can be spontaneously generated for the power data transactions. Digital authentication is used in the transaction method. The service center agency is established at each node for energy transactions, which ensures the fairness of transactions to a great extent.

(2) Contract Layer

The contract layer includes power transaction requests for the execution of smart contracts. In essence, the smart contract is to trigger the expected set conditions and deploy the blockchain code in accordance with the running state to automatically execute the relevant requests. As part of the power data that requires protection, the smart contract acts as a bridge between the blockchain and the user side, to achieve client information invocation and interaction with the underlying blockchain. Besides, all blockchain nodes can play a role in transaction restrictions in a certain order.

(3) Consensus Layer

The consensus layer is designed for confirming the transactions and reaching a consensus. Here a pluggable design is used. An appropriate consensus mechanism can be selected according to the actual application scenario. In the power data transaction scenario set in this paper, substation nodes in the power region are small in quantity, and the blockchain network is not very large in scale. Also, authentication through CA is required at each node, and the groups present a trust relationship with each other. For this reason, the nodes are all implemented within a relatively trusted private execution environment.

(4) Network Layer

The network layer is designed to encapsulate the network topology, message propagation protocol, and data validation mechanism in the blockchain system. In this design, the communication mechanism is used to meet the requirements related to power data transactions, thereby changing the network topology.

(5) Data layer

The data layer involves the local ledger of the substation nodes, which includes blockchain transaction information and power data information. The transaction information of the block is stored on a specific block, and the block transaction information can only be used for query and addition but not for modification and deletion, which makes the power data cannot be tampered with at will. The state database stores the latest values of the variable keys in the transaction, and the power data can be queried in real-time in the current state of the power data. In the blockchain network, the substation nodes with the same channel have the same ledger. In doing so, the risks of illegal data tampering or data center being attacked that may occur in the

traditional centralized data storage can be avoided, and thus the security of power data can be enhanced.

4.2.2 State Synchronization Mechanism of Smart Contracts

In practical applications, the environment of each node on the blockchain system is different. If the network latency and node hardware performance are different, the speed of smart contracts running at the nodes will be different. The logic structure of these smart contracts themselves is relatively complex, and their states of existence will change in the operation of different stages. Given this, if you want to better maintain the consistency of the state of the nodes, the transaction needs to be accelerated. But this is also a major problem faced in the current practical applications. Therefore, this paper proposed smart contracts.

When multiple complex smart contracts in the power data transaction center require a long execution period, and if it is executed under different nodes, the execution speed will be significantly different due to the difference in production conditions and environment, which also promotes the synchronization of the contract execution state, the smart contracts can be divided into several stages. The data state will change after the execution of the contract under different stages, so it is necessary to add a state synchronization collector.

In the execution of smart contracts, the state synchronization mechanism will shorten the transaction delay. The phased execution of smart contracts can realize the execution of each commitment, ensure transaction correctness, and promote the timeliness of blockchain transactions.

4.2.3 Experimental Scheme Implementation

According to the power data storage scheme, the specific scheme implementation process is shown in the figure. The power transaction request will be sent through the client, and the client's application server will invoke the SDK interface according to the request type after receiving the request. Automatic data transaction is realized through the smart contract. The SDK needs to verify the identity of the CA node before the transaction. When the verification is passed, the interaction with the blockchain can be realized. Then the transaction is executed, and the transaction state is updated.

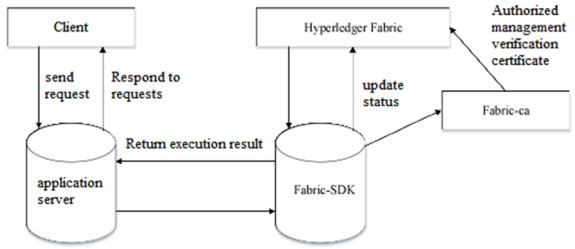

Fig. 5 Scheme Execution Flow

References

1. Carvalho Arthur, Merhout Jeffrey W., Kadiyala Yogesh, Bentley II John. When good blocks go bad: Managing unwanted blockchain data[J]. International Journal of Information Management, 2021, 57.
2. Seithikurippu R. Pandi-Perumal,Sagar Santaji,Veena V. Desai,Thankam Sunil,Vijay Kumar Chattu. The Blockchain Never Sleeps: How Can Blockchain Technology Transform Sleep Medicine?[J]. Sleep and Vigilance, 2021(prepublish).
3. PérezSánchez María de los Ángeles,Tian Zhuowei,BarrientosBáez Almudena,GómezGalán José,Li Hanliang. Blockchain Technology for Winning Consumer Loyalty: Social Norm Analysis Using Structural Equation Modeling[J]. Mathematics, 2021, 9(5).
4. Mila Jasper. Air Force Buys Streaming Data Warehouse for Pathfinder, JADC2 Concepts[J]. Nextgov.com (Online),2021.