A method and system for unified authentication management and control of power secondary equipment based on blockchain

Liming Wang [1], Rao Fu [2], Zhongxing Fu [3], Jiawei Sun [4]

[1] State Grid Jiangsu Electric Power Co., LTD., Nanjing 210002, China
[2] Xuzhou Power Supply Branch of State Grid Jiangsu Electric Power Co., LTD., Xuzhou 221000, China
[3] Yancheng Power Supply Branch of State Grid Jiangsu Electric Power Co., LTD., Yancheng 224000, China
[4] Nanjing Power Supply Branch, State Grid Jiangsu Electric Power Co., LTD., Nanjing 210002, China

Abstract. Blockchain technology is an advanced database mechanism that allows transparent sharing of information across corporate networks. By analyzing the insufficiency and improvement plan of the operation and maintenance safety management of power secondary equipment, it is proposed to use the operation and maintenance management and control system to select EOS as the underlying scheme of the blockchain, and discuss it based on a trusted blockchain network system.

Keywords: Blockchain, trusted system, decentralization, authentication control, equipment operation and maintenance.

1. Preface

The safety management and control of power secondary equipment in the process of operation and maintenance of power grid companies and the prevention of unauthorized access, illegal operations, malicious intrusion and other security risks in the process of operation and maintenance is a crucial task. With the rapid development of my country's economy and the significant enhancement of social productivity, the power grid is transforming and upgrading in the direction of distributed, clean and low-carbon, digital and intelligent; Gaining political and economic interests has become its main driving force, resulting in a dramatic increase in the destructiveness of attacks. The cyber black industry chain is gradually taking shape, and more attacks are directed to key information infrastructure in important industries such as government agencies, energy, finance, transportation, and communications. The power system is even more frequent. Power systems such as Ukraine and Venezuela have been repeatedly attacked by cyber attacks or blackmailed by viruses. The light ones cause economic losses to enterprises, and the heavy ones cause large-scale power outages that seriously affect social and economic operations. Cyber security has become a problem faced by the power system. real threat. At present, there are 14 dispatching agencies above the prefecture level, more than 400 power plants, and more than 3,000 substations within the jurisdiction of Jiangsu Province. Main station, substation, power plant network-related secondary equipment operation and maintenance and maintenance process of personnel identity lack of verification, "super administrator" account authority is difficult to control, authority leakage in the process of operation and maintenance and maintenance, etc. Externally imported risks" are becoming increasingly serious. In this context, the requirements of the power monitoring system for the degree of intelligence and networking are gradually becoming higher, and the requirements for the safety management and control of the operation and maintenance of power secondary equipment are also constantly improving. [1]

On October 24, 2019, General Secretary Xi Jinping pointed out during the 18th collective study of the Political Bureau of the CPC Central Committee that the integrated application of blockchain technology plays an important role in the new technological revolution and industrial transformation. We should take blockchain as an important breakthrough for independent innovation of core technologies, clarify the main direction of attack, increase investment, focus on conquering a number of key core technologies, and accelerate the development of blockchain technology and industrial innovation. On April 20, 2020, the National Development and Reform Commission clarified for the first time three aspects of new infrastructure, among which information infrastructure includes new technology infrastructure represented by artificial intelligence, cloud computing, and blockchain. In the process of promoting the transformation and development of the power grid, the blockchain technology meets the development needs of the energy Internet, which is conducive to promoting the transformation of the production management and operation mode of the power grid to an intelligent and

networked direction, and has a positive effect on the adjustment of the power grid industrial structure.

Blockchain technology has the technical characteristics of decentralization, multi-party participation, openness and transparency, traceability, and anti-tampering. It has been used more and more in power business scenarios. However, at present, there is no research and application based on blockchain technology to solve the insufficiency in the safety management and control of power secondary equipment operation and maintenance. This system applies the features of decentralization, security, trustworthiness, traceability, and easy auditing of the blockchain system to the safety operation and maintenance management and control of power secondary equipment, and proposes a blockchain-based power operation and maintenance safety supervision and emergency method. Realize unified authentication management and control technology for power secondary equipment based on blockchain. By building a blockchain network, combined with biometric technology to build a digital identity for operation and maintenance. Based on the TACACS+ protocol, the decentralized AAA service can be realized, and the key can be distributed through the blockchain network to realize the key management strategy of "one case, one encryption". At the same time, the entire business process information is uploaded to the chain, providing traceability and supervision of the operation and maintenance business, and ensuring the openness and transparency of the supervision process. The project plan utilizes the characteristics of blockchain traceability and difficult to tamper to realize penetrating management of the operation process of power safety operation and maintenance, realize strong supervision of safe production, support the innovative development of the power industry, and ensure the safe and stable operation of the power grid. [2-4]

2. Technical Architecture

The technical architecture is shown in Figure 1.

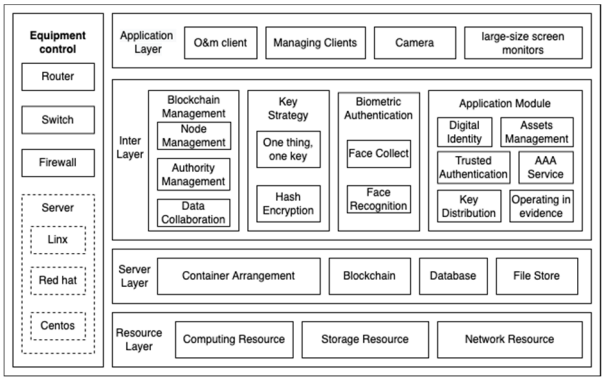

Fig.1 Technical Framework

Resource layer: Provide the infrastructure resources for the operation of the system, mainly related computing resources and storage resources provided by the server. The network resources need to be applied for and configured in combination with the three areas of the power system and the actual situation of the external network. The client needs to be installed and deployed on the user's personal computer and configured with the corresponding camera device.

Service layer: The server part of the system is packaged and deployed using container technology. The service dependencies of the system also include blockchain, database, and file storage.

Middle layer: The middle layer implements the core logic part of the system. This part mainly includes blockchain management, key management strategy, biometric authentication and main application modules.

Application layer: The system is given to users through the corresponding client. There are mainly operation and maintenance clients for operation and maintenance personnel, and management clients for management personnel.

Device management and control: The system implements AAA services and connects to mainstream network devices, including routers, switches, and firewalls, through the TACACS+ protocol. It also supports server systems, such as Meditation, Centos, and Redhat. [5-7]

3. Digital Authentication Design

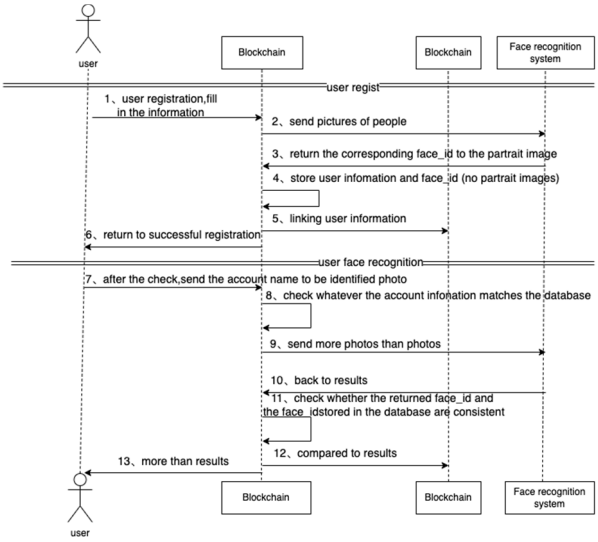

Fig. 2 Digital Identity Identification

Table 1. Digital identity information

field name	type
face_id	Unit64
name	String
job_number	String
full_name	String
phone_number	String
id_card	String
company	String
position	String
role	Int32
name_hash	Checksum256
password_hash	Checksum256

The premise of safety management and control is to include operation and maintenance personnel and secondary power equipment into system management. Compared with traditional management solutions, this system uses blockchain smart contracts to build decentralized digital identities for both operation and maintenance personnel and power secondary equipment. The system will centrally manage personnel and equipment based on digital identities.

When operation and maintenance personnel and management personnel use the corresponding client to log in to the system, they need to connect the camera and perform face recognition before logging in. Managers will create digital identities for operators. Digital identity information will be stored through smart contracts on the blockchain. The original avatar image of the operation and maintenance personnel will be stored in the face recognition system, and the corresponding image hash value will be stored in the digital identity on the chain. When the operation and maintenance personnel use the digital identity through the operation and maintenance client, the face recognition technology will obtain and verify the face image according to the digital identity chain to carry out safe and reliable authentication. The entire digital identity verification process will be stored on the chain at the same time, effectively solving the problem of "inconsistency between people and tickets". [8-10]

4. Decentralized AAA service design

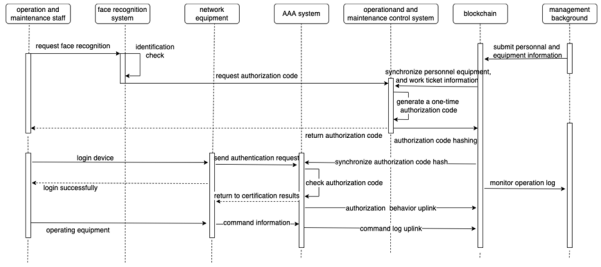

Fig. 3 The Sequential Process

The management personnel enter the operation and maintenance personnel and equipment information into the system through the management background, and record it on the blockchain.

The operation and maintenance personnel request face recognition through the operation and maintenance client, and the face recognition system is verified through the personnel system records.

After the face recognition verification is correct, an application will be sent to the operation and maintenance management and control system to request a one-time authorization code.

The operation and maintenance management and control system generates a one-time authorization code based on personnel permissions, returns the plaintext of the authorization code to the operation and maintenance personnel, and saves the hash ciphertext of the authorization code on the chain.

The blockchain network will synchronize the authorization code hash ciphertext to all nodes.

Operation and maintenance personnel use their own account name and the authorization code just applied to remotely log in to the specified device.

The device sends the authentication request to the AAA server through the TACACS+ protocol.

The AAA server will query and verify the ciphertext of the authorization code submitted by the user from the blockchain, return the authentication result, and record the authentication behavior on the chain.

The device receives the verification result. If the verification is correct, the user has successfully logged in and can proceed further.

The device uploads the command information of the user's operation to the chain and saves it as the user's operation record.

The unified certification and control technology of power secondary equipment is the key realization of the system. The technical solution will connect multiple systems in the power system, such as the network management system, work ticket system, personnel database system, and face recognition system, to provide blockchain-based AAA services for power secondary equipment.

As shown in Figure 3, this scheme designs a secure and credible password distribution strategy, and provides decentralized AAA services by combining blockchain technology and TACACS+ protocol.

Based on the digital identity contract, this scheme builds a rights management contract to further manage the rights of operation and maintenance personnel. The rights management contract can group the operation and maintenance personnel and power secondary equipment, and restrict the operation and maintenance personnel to only access the equipment in the corresponding group. When the AAA service verifies the user's login information, it will also check whether the device has access rights. When the operation and maintenance personnel are operating, they can request elevated permissions to obtain more advanced device operation permissions. The operation and maintenance personnel apply to the management system for the login authorization of a certain device, and the system will generate a one-time random high-strength password for the operation and maintenance personnel. The plaintext of the password will be pushed to the dedicated client of the operation and maintenance personnel, and the hashed ciphertext corresponding to the password will be stored on the chain and broadcast to each node with the blockchain network.

The TACACS+ protocol is a TCP-based access control protocol for network devices that provides authentication, authorization, and accounting services. The so-called 3A means Authentication, Authorization, and Accounting.

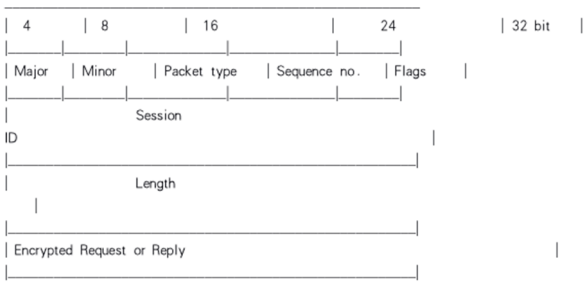

Fig. 4 Protocol Message Structure

Major Version—the main TACACS+ version number.
Minor Version - minor TACACS+ version number. Modifications to the TACACS+ protocol are permitted when necessary to maintain backward compatibility.
Packet Type - possible values include:
TAC_PLUS_AUTHEN:= 0x01 (authentication);
TAC_PLUS_AUTHOR:= 0x02 (authorization);
TAC_PLUS_ACCT:= 0x03 (Billing).
Sequence Number - the sequence number of the data packets in the current session. The sequence number of the first TACACS+ packet in the session must be 1, and the sequence number of each subsequent packet must be incremented by 1. So the client only sends packets with odd sequence numbers, while the TACACS+ Daemon only sends packets with even sequence numbers.
Flags - This field includes flags in various bitmap formats. The Flag value indicates whether the data packet is encrypted.
Session ID - the ID of the TACACS+ session.
Length—The total length of the TACACS+ packet body (excluding the header).
TACACS+ is actually a brand new protocol. TACACS+ and RADIUS have replaced earlier protocols in existing networks. TACACS+ uses Transmission Control Protocol (TCP), while RADIUS uses User Datagram Protocol (UDP). Some administrators recommend using the TACACS+ protocol because TCP is more reliable. RADIUS combines authentication and authorization from a user perspective, while TACACS+ separates these two operations.
The system implements a service node that implements the TACACS+ protocol in combination with blockchain technology. The AAA server corresponding to all managed devices will be configured as the service node IP. When the O&M personnel use the one-time password to log in to the device remotely, the device will submit the authentication request to the corresponding TACAS+ service node. The service node will query the ciphertext in the blockchain contract to confirm the login authentication request. After the verification is correct, the corresponding authentication result will be returned, allowing the operation and maintenance personnel to log in to perform related operations. At the same time, the service node will delete the corresponding one-time password ciphertext in the contract to ensure that the password will not be reused.
The system solution provides a "one-for-one secret" key generation and distribution strategy for temporary operation and maintenance personnel and resident operation and maintenance personnel of the work ticket system. At the same time, combined with the decentralization characteristics of the TACACS+ protocol and the blockchain, a decentralized unified authentication control technology is realized.

5. Trusted operation log design

This system uses EOS as the underlying scheme of blockchain, EOS is the first blockchain operating system, which provides database, database schema and multiple indexes for applications to process and store data easily. It provides account permissions and a full set of account functions, account recovery, handles complex scheduling of multiple tasks across CPUs and even clusters, handles all authentication and key management so that you can focus on business logic rather than reimplementing a cryptographic system. Handles all Internet program communications. EOS enables developers to focus on building the applications that users need, with no mandatory gas, and greatly speeds up the process for developers to build applications on top of it.

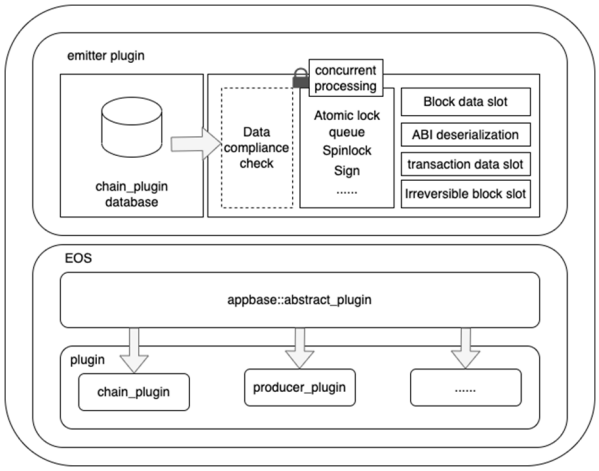

Fig. 5 Data Collaboration

The user system monitors the transaction transaction data through the emitter_plugin;
Emitter_plugin obtains the transaction data signal through the transaction signal slot;
The plugin obtains the transaction pointer from EOS;
The Emitter_plugin plugin checks the data legally;
The plug-in deserializes transaction transaction data through abi;
Put the data back into the chainbase database to get the chain plugin data;
Plugins process concurrent data queues;
Trigger user business system and push transaction data.
Since the AAA service is configured, all user commands and operations will be sent to the AAA service node in real time. The AAA service node stores the user's operation log invoking the log certificate storage contract on the chain. Blockchain is naturally a trusted log service system. Based on the non-tamperable and traceable features of the blockchain, certified logs can be provided to on-chain contracts and off-chain systems for real-time analysis, processing and post-event traceability.

Operation log process traceability and compliance verification refer to the operation and maintenance operations performed by the operation and maintenance personnel in the unified authentication service, and the operation log will be collected and stored using the blockchain.

This system deeply combines the TACACS+ protocol and blockchain technology, and uses the TACACS+ protocol to collect the operation command records of the operation and maintenance personnel on the equipment, and store the operation records on the chain. The management system will synchronize the operation and maintenance operation logs of the entire network into the system through the on-chain and off-chain data collaboration module (as shown in Figure 5) for collection and processing.

Blockchain technology ensures the authenticity and validity of operation logs. With the technical support of on-chain and off-chain data collaboration, the process traceability and supervision of all operation and maintenance operation logs can be realized. This technology will re-collect and organize logs off-chain, generate corresponding reports, and provide a reliable basis for operation and maintenance supervision.

6. Project achievements and applications

As shown in Figure 6, it is the deployment topology of the system. At present, the system has supported 19 different types of devices of H3C, HUAWEI, ZTE and other brands. According to the topology shown in the figure, the demonstration application was conducted in Jiangsu Province by the State Grid.

Through the research on key technologies such as operation and maintenance digital identity authentication, operation and maintenance security management and control, operation and maintenance event supervision and emergency response of the power monitoring system based on the blockchain, this system solves the problems in the operation and maintenance process, such as difficulty in controlling the authority of super accounts, inconsistency of people and tickets, etc. Problems, timely discovery of various dangerous operations and attack threats in the operation and maintenance process. A prototype of a blockchain-based operation and maintenance management and control system for power secondary equipment has been formed, including a blockchain-based operation and maintenance personnel digital identity management module, a biometric-based unified authentication management and control module, and a decentralized AAA service module based on the TACACS+ protocol. The operation and maintenance operation safety monitoring module based on on-chain and off-chain data collaboration and the smart contract-based emergency response module for dangerous operations can comprehensively improve the network security operation and maintenance and automated management level of the power monitoring system. [11-12]

7. Conclusion

By studying the power network security digital identity authentication and control system based on the blockchain, with the help of the distributed consensus characteristics of the blockchain, the power network security digital identity and its authentication system can be realized, and the whole process of operation and maintenance can be stored on the chain to realize intelligent Chemical supervision and emergency response. On the one hand, this system can solve the actual problems in the current operation and maintenance business, and on the other hand, it can closely integrate the emerging technology of blockchain to further improve the company's ability to independently innovate core technologies.

This system has many meanings, mainly reflected in the following aspects:

(1) The establishment of a digital identity system for blockchain storage will help to realize an integrated authorization and authentication system.

Digital identity is a multi-dimensional digital identity such as the authority and attributes of operation and maintenance personnel. Based on the non-tamperable and traceable properties of blockchain, it can ensure the validity of personal information, improve the credibility of digital identity, and break through the overall situation based on blockchain. The unique, high-availability, parseable, and encrypted and verifiable decentralized digital identity technology for personnel provides reliable identity support for security operation and maintenance management.

(2) The unified authentication management and control technology of power secondary equipment based on blockchain is helpful to realize the integrated, fine-grained and dynamic authorization and authentication system of power system operation and maintenance.

Combined with the digital identity of the decentralized personnel, a blockchain-based decentralized secondary equipment unified authentication management and control technology is constructed to provide "one secret" operation and maintenance security management and control for power secondary equipment, and to ensure the safe and reliable operation of the operation and maintenance personnel. and log traceback.

(3) On-chain and off-chain data collaboration based on smart contracts helps to achieve rapid isolation of dangerous operation behaviors and intelligent operation and maintenance security control.

Through the deployment of smart contracts, the collaborative analysis of on-chain operation and maintenance records and off-chain operation results is realized. Based on the non-tamperable characteristics of the blockchain, the traceability and supervision of the operation and maintenance process are realized. Research the emergency response technology for dangerous operation of power operation and maintenance, combined with the operation information on the chain, through the decentralized digital identity system, the rapid isolation of dangerous operation behaviors, and the realization of intelligent operation and maintenance safety management and control. [14-15]

This work was supported by the Science and Technology Project of State Grid Jiangsu Electric Power Co., Ltd., project number J2021021.

References

1. Zhang Ning, Wang Yi, Kang Chongqing, et al. Blockchain technique in the energy Internet: preliminary research framework and typical applications[J]. Proceedings of the CSEE,2016,36(15):4011-4023.
2. She Wei, Bai Menglong, Liu Wei. Architecture of The Energy Blockchain. Application And Development Trend. Journal of Zhengzhou University (Science Edition), 2021, 53(4): 1-21.
3. Jiangsu Electric Power Test and Research Institute Co. LTD. The utility model relates to a power data storage method and power data sharing method based on blockchain: CN202110348024.6[P]. 2021-06-11.
4. Yuan Yong, Wang Fei- Yue. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42 (4): 481-494.
5. Li Zeke, Chen Zewen, Wang Chunyan, et. Network security threat tracing technology of power monitoring system[J] . Electric Power Engineering Technology, 2020, 39 (2): 166 - 172
6. Wang F Y, Zhang J, Wei Q L, Zheng X H, Li L. PDP: parallel dynamic programming[J]. IEEE/CAA Journal of Automatica Sinica, 2017, 4(1): 1-5.
7. Xu Ye. My country's blockchain research and development application status and development suggestions[J]. Science and Technology China,2019(5):13-15.
8. Cao Hongli, Huang Zhongyi. Blockchain: the infrastructure of building digital economy[J]. Cyberspace Security,2019,10(5):75-81.
9. Yang Dechang, Zhao Xiaoyu, Xu Zixiao, et al. Developing status and prospect analysis of blockchain in energy internet[J]. Proceedings of the CSEE, 2017, 37(13):3664-3671.
10. Liu Guangyi, Zhu Wendong, Chen Jinxiang and Zhang Yi. Characteristics, Application Scenarios and Analysis Platform of Smart Grid Big Data[J] . Southern Power System Technology, 2016, 10 (5): 102 -110.
11. Wang Xinyan, Jiang Wei, Qin Long. Application of power system security evaluation management system using blockchain technology[J]. Electric Power Information and Communication TechnoloTechnology,2020,18(6):68-74.
12. Zha Xuan, Cui Xiaofei, Wei Liang, et al. Security analysis and protection of blockchain infrastructure[J]. Information and Communicationa Technologies,2019, 13(6):28-33,58.
13. Jiang Haitao, Wang Xiang, Li Zhi, et al. Research and application of power system security evaluation management sys-tem based on blockchain[J]. Electric Power Information and Communication Technology,2020,18(1):67-73.
14. Jin Cheqing, Zhang Zhao, Pan Bin. Blockchain: infrastructure of new-generation Internet[J]. Journalof Xinjiang Normal University (Edition of Philosophyand Social Sciences),2020,41(5):103-113,2.
15. Xu Meiqiang, Gao Zhiyuan, Wang Wei, et al. Smart substation configuration version management based on blockchain technology[J]. Power System Protection and Control,2020,48(2):60-67.