Privacy Protection of the Smart Grid System Based on Blockchain

Siyuan Liu¹*, Qiong Zhang² and Honggang Liu³

¹School of Control and Computer Engineering, North China Electric Power University, Baoding, China
²Guodian NARI Technology Co., Ltd., Nanjing, Jiangsu Province, China
³Information and Communication Branch of Chongqing Electric Power Company of State Power Grid, Chongqing, China

*Corresponding author e-mail: 40550998@ncepu.edu.cn

Abstract. With the development of new technologies for smart grid construction, the smart grid is gradually developing. Smart grid construction is an important field of next generation information technology, and its value and significance have been widely recognized. Smart grid construction not only provides development opportunities, but also brings great challenges. Security and privacy have become serious problems in the development of smart grid. Based on this, this paper discusses the system structure of the block chain, and puts forward the security diagnosis scheme of the smart grid according to the existing problems in the smart grid. Based on the theoretical basis of smart grid big data technology, this paper combines the grid data encryption process with the privacy protection process under the premise of protecting privacy and security, and develops the latest network security protocol. Then use block chain distributed storage to reduce the connection protection process in privacy, and use multi-level encryption. The experimental results show that the technology can improve the rate of sensitive data hiding and has good anti-cracking ability, which provides a theoretical reference for the construction of enterprise power grid.

Keywords: Smart Grid, Privacy Protection, Big Data Technology, Safety Diagnosis

1. Introduction
Smart grid is the intelligence of the grid [1,2]. It is based on an integrated high-speed two-way communication network. Through the application of advanced sensor measurement technology, advanced equipment technology, advanced control methods and advanced decision support system technology, the goal of reliable, safe, economical, efficient, environmentally friendly and safe use of the power grid has been achieved [3-4]. Its main features include self-healing, encouraging and protecting users, resisting attacks, providing power quality that meets the needs of users in the 21st century, allowing access to various forms of power generation, starting the power market, the optimizing and operating assets efficiently. Smart grid [5] includes three processes of power
transformation, transmission and distribution. The electric energy is produced from the power plant, enters the high-voltage transmission line through the transformation and voltage rise, and then distributes the power to each user. The high-voltage transmission part is also called the main network, and the low-voltage distribution part is also called the distribution network [6].

Block chain is a mode of building and managing transaction processing through transparent and trusted rules in the peer-to-peer network environment [7,8]. It has distributed peer-to-peer, chained data block and defense. It has the characteristics of anti-counterfeiting, anti-tampering, transparent, reliable and high reliability [9]. Block chain is divided into public block chain, joint block chain and private block chain. Decentralization is the most prominent and essential feature of block chain. Secondly, block chain also has the characteristics of openness, independence, security and anonymity [10]. Block chain has great potential application value in the fields of finance, Internet of things and logistics, public service, digital copyright, insurance and public welfare.

Combined with the unique technical characteristics of block chain, this paper proposes an intelligent grid information security scheme based on block chain. The purpose of this paper is to effectively solve the main problems of data management, trust, security and privacy in the development of modern grid. The block chain security plan provides trust, proprietary records, transparency and connectivity support for the grid, identifies the coordination of flexible devices, builds an efficient and secure distributed grid network, and distributes a large number of data security systems to effectively protect user privacy types.

2. Smart Grid and Block chain System Structure

2.1 Smart Grid System Structure

Power grid business data is mainly divided into grid operation data, management data, power enterprise marketing data and monitoring data. In the actual operation of the power system, big data is widely used in all aspects, which can produce more data. Smart grid big data has the characteristics of large amount of data, low value density and many data types. These characteristics promote the relevant information in big data, and gradually appear within the enterprise, forming the agglomeration effect. The existing big data technology solutions for smart grid can only be used to support data aggregation calculation. Therefore, it is necessary to study the big data analysis and mining technology of smart grid based on privacy protection. The data in the smart grid is regarded as a trusted third-party sequence, and the security protocol of local website is used to transfer the data with the third party. The transfer function is as follows:

$$ e = \prod_{p(j) \in s} c(B_i,k)^{-1} $$  \hspace{1cm} (1)

In the formula, $e$ is the security sequence of smart grid; $p(j)$ is all the third-party data; $s$ is the security protocol; $B_i$ is the data item set; $k$ is the block chain safety factor, which is only introduced in this calculation, without directional analysis; $c$ is the aggregation characteristics of smart meter data.

If the third-party data aggregation feature $c$ function is maintained, some attributes of the data can be retained. Then use the support of modern grids to improve the security of smart grids. The calculation formula of protocol support is as follows:

$$ w(j) = \sum A e $$  \hspace{1cm} (2)

Where $w(j)$ is the support degree of secure line and $A$ is the secure transaction data set.

According to the relevant requirements for blockchain support, in the mining function of big data association rules in the smart grid, $w(j) \Rightarrow x$ is the minimum data adjustment coefficient used for mining, and has nothing to do with data loss and mining costs in large grids.
Where $F$ is the big data association rule of smart grid; $B_0$ is the decryption constant of block chain; and $F(t)$ is the total amount of private data of smart grid mined in time $t$.

2.2 Block Chain System Structure

In this paper, a data transmission mechanism based on security sovereignty block chain monitoring is established in the smart grid between users and power companies to achieve data security and transparency. The smart grid network includes regional chain network, processing and coordination nodes, smart contract center and registration and certification layer. Users can register the system by visiting the interface and provide necessary information. The information is submitted to the smart grid network and received and processed in the registration and authentication layer. The data of users registered on the system are first received by the verification program. Processing the request generates a unique ID for the user, which identifies each user on the system. The power company directly interfaces with the data processing and monitoring layer, and transmits the recorded data of distribution operation to the data processing and monitoring layer according to the request of processing and negotiation nodes.

3. Experimental Background and Parameter Setting

In recent years, with the expansion of the application scope of smart grid, the research on the security performance of smart grid is becoming more and more important. There are a lot of communication data with complex structure and abnormal form in the smart grid. If there are loopholes or errors in the transmission process, the big data structure of the power grid will tend to be infinitely complex and reduce the power generation efficiency of the smart grid. Therefore, privacy protection of smart grid is extremely necessary. This paper proposes a big data privacy protection technology based on block chain by taking advantage of the relevant advantages of block chain. In order to reduce the confidentiality of information, smart grid information is a rule of the association, and encryption functions of various denominations are used in several blocks. With the help of block chain distributed storage mode, the communication volume in the process of privacy protection is reduced, and the key generation time and encryption time are effectively shortened. The minimum support degree $F_{\text{min}}$ and the maximum confidence degree $F_{\text{max}}$ of data association rules are set as constant functions; the switching state of smart grid is taken as the criterion to record the binary form of $F_{\text{min}}$ and $F_{\text{max}}$. In this paper, three $F_{\text{min}}$ and $F_{\text{max}}$ values are selected for comparison. Among them, "1" indicates that the smart grid is in the closed state; "0" indicates that the smart grid is in the power-off state. The binary form of the smart grid switch state is shown in Table 1.

| Thread | Transformer substation | Watt-hour meter | Interactive terminal | Monitor |
|--------|------------------------|-----------------|----------------------|---------|
| $F_{\text{min}} (1)$ | 1 | 1 | 1 | 0 |
| $F_{\text{min}} (2)$ | 0 | 1 | 1 | 0 |
| $F_{\text{min}} (3)$ | 0 | 0 | 1 | 0 |
| $F_{\text{max}} (1)$ | 0 | 0 | 1 | 1 |
| $F_{\text{max}} (2)$ | 0 | 0 | 0 | 1 |
| $F_{\text{max}} (3)$ | 1 | 1 | 1 | 1 |

4. Discussion
The experimental verification of big data privacy protection technology based on block chain is conducted from two aspects: data privacy protection ability and execution efficiency of smart grid. The privacy protection capability of data is guaranteed based on the security of block chain technology, while the execution efficiency of smart grid is verified from the privacy protection time and traffic volume of the technology. In order to verify the superiority of the privacy protection technology proposed in this paper, the traditional technology is used for comparison, and the differences of data privacy protection ability and execution efficiency of smart grid between different technologies can be obtained.

4.1 Sensitive Data Hiding Rate

The encryption ability of the privacy protection technology based on block chain is mainly reflected in that no entity except the user can accurately obtain the decrypted user data, so it uses the sensitive data hiding rate to calculate. The experimental results are shown in the figure below.

![Figure 1. Comparison of sensitive data hiding rate](image)

From the data in Figure 1, we can see that the sensitive data hiding rate of privacy protection technology in this paper is higher than that of traditional privacy protection technology, especially when the data set is 50. The analysis shows that the privacy data hiding rate of the privacy encryption technology in this paper will not decrease with the increase of the total data volume, because the privacy protection technology in this paper focuses on the processing of a large number of data, while the traditional technology mainly focuses on the privacy management of cloud data. Therefore, from the perspective of the hiding rate of sensitive data, we can see that this privacy protection technology has advantages.

![Figure 2. Comparison of anti-cracking rate of sensitive data](image)
4.2 Comparison of Data Anti-cracking Rate

In order to further verify the performance of different privacy protection methods, it is necessary to compare the anti-cracking rate of privacy data encryption, and the results are shown in the figure above.

According to the data in Figure 2, the anti-cracking rate of the traditional privacy protection technology is about 65%, while the anti-cracking rate of the privacy protection technology in this paper is always kept at about 96%. The anti-cracking ability is good, which effectively improves the security of cloud information data encryption storage. From the aspect of anti-cracking rate of smart grid privacy data, this technology has certain advantages, its anti-cracking rate is higher than the traditional technology, and the data processing ability is strong. There is a big difference between the two technologies in the anti-decryption rate of data, and this paper has obvious advantages. At the same time, the privacy protection technology in this paper can use the block relationship between data to better classify and encrypt the private data, so it can realize the privacy protection of big data in all aspects of smart grid.

4.3 Safety Analysis and Performance Evaluation

The private key is not exchanged between the receiver and the private key in the whole process of decryption. Even if the attacker monitors the communication channel, each user will use signcryption algorithm to signcrypt power multidimensional data before publishing it. The ciphertext is transmitted in the channel. Even if the attacker intercepts the ciphertext, it can't decrypt the corresponding plaintext, so the attacker can't get the multi-dimensional data of consumers. In CBSG, there is no need for key transmission, and the user data and smart grid monitoring policies collected by the smart meter end are recorded on the alliance block chain, and the confidentiality of the data can also be ensured through the block chain. The privacy protection technology in this paper is based on the alliance chain technology. The data of each node is recorded in the existing master node in the useless permanent block chain. Therefore, once a new block is created, its data integrity can be verified. In the process of multi-dimensional data publishing, the attacker cannot forge a new signature through the stolen signature, which can resist the forgery attack and ensure the integrity of the user's power data in the transmission process.

The privacy registration method used in this article may collect comprehensive information and send it to multiple recipients. Each recipient receives the corresponding field by calculating the "segment" index. Grid operators and equipment suppliers process multi-dimensional data to understand the regulation and control of the smart grid. By summarizing user power consumption data, user anti-theft management functions, key user control and data maintenance tasks can be realized, and energy management efficiency data can be recorded in the collaboration chain. In addition, the chain of lockdown is permanent. Once the information is stored in the blockchain, it can be stored permanently, that is, the information is permanent. After checking the user's electricity data, the grid operator will prepare a smart contract based on each user's energy consumption. Verify a user's power regulation through modern contracts. At the same time, the equipment provider will monitor the status of the equipment to ensure the normal operation of the power supply and save network construction costs.

The structure of regional chain system is to add some specific codes required by enterprises in the relevant documents when publishing electronic documents, and then use the identity of the publisher to identify the relevant documents, so as to increase the recognition power of relevant documents. During the transfer process, the judge should determine whether the document has been used or violated by other organizations. At this time, the signature of the document can be verified through the regional chain system structure, so as to ensure the security of the whole document. From the use characteristics of the regional chain system structure, this technology is mainly to maintain the correctness and integrity of documents in a specific time. Especially for the construction of enterprise smart grid big data system, we should actively adopt the regional chain system structure to ensure that the system is subject to external interference and protect the data from the interference of the
document itself. At present, when the regional chain system structure is widely used, when internal users access the relevant network and big data system for data query and other operations, it can provide users with effective and correct information. When users cut into the related system, they need to sign before they can log in to the corresponding system. Under this operation, it can effectively prevent some shameless elements from intruding into the system for data theft when users enter the database, so as to ensure data security from the aspect of user identity authentication.

5. Conclusions
The privacy discussion was established behind the gradual development of the modern grid. In the process of technology research and development, we need to focus on protecting user privacy information, focusing on the application of large-scale data analysis and mining technology. It has a new impact on user privacy information, especially in the ongoing grid expansion. In order to achieve good security, the application of smart grid data analysis and mining technology is essential. Experiments show that this technology can increase the speed of hiding sensitive information and has good anti-leakage capabilities. Therefore, in the process of privacy protection of smart grid big data, the block chain technology proposed in this paper has better privacy protection ability and actual encryption ability, which is suitable for data protection of smart grid.

References
[1] Min, X. , & Ting, Z. Research on big data analysis and mining technology of smart grid based on privacy protection. Electronic Test, 2019, 12(042), 17-25.
[2] Bo, C. , Zhuying, Z. , Zheng, W. U. , & Hui, Y. Research and application of privacy protection technology in smart grid. Computer & Digital Engineering, 2017, 46(19), 13-15.
[3] Li, D. , Liu, W. , Deng, L. , & Qin, B. Design of multimedia block chain privacy protection system based on distributed trusted communication. Transactions on Emerging Telecomunications Technologies, 2020, 19(4), 56-59.
[4] Kim, S. M. , Lee, T. , Kim, S. , Park, L. W. , Park, S. , & Wan, X. Security issues on smart grid and block chain-based secure smart energy management system. MATEC Web of Conferences, 2019, 260(29), 76-79.
[5] Garlapati, S. Block chain for iot-based nans and hans in smart grid. arXiv e-prints, 2020,10(16), 45-49.
[6] Son, Y. B. , Im, J. H. , Kwon, H. Y. , Jeon, S. Y. , & Lee, M. K. Privacy-preserving peer-to-peer energy trading in block chain-enabled smart grids using functional encryption. Energies, 2020, 13(6), 13-21.
[7] Ocha, I. S. , Silva, L. A. , Mello, G. D. , Garcia, N. M. , Santana, J. F. D. P. , & Leithardt, V. R. A cost analysis of implementing a block chain architecture in a smart grid scenario using sidechains. Sensors (Basel, Switzerland), 2020, 20(3), 98-100.
[8] Chunlin, Y. , Na, Z. , Zhengyun, F. , Yannining, C. , Zheng, Y. , & Ledi, L. An enterprise credit evaluation method for power grid service providers based on block chain is presented. Journal of Physics: Conference Series, 2020, 1437(1), 012-021.
[9] Sheng, ZHONG, Xinyi, & HUANG. Special focus on security and privacy in block chain-based applications. Science China(Information ences), 2020,v.63(03), 5-6.
[10] Wang, D. , Zhao, J. , & Wang, Y. A survey on privacy protection of block chain: the technology and application. IEEE Access, 2020, 11(99), 1-6.