Privacy Protection Method of Electric Power Network Based on Blockchain

Maolin Zhang¹,*, Weihua Zhao¹, Wei Shi², Haiming Zhou²

¹Kunming Power Exchange Center Co. Ltd. Kunming, Yunnan, 650000, China
²Insigma Hengtian Software Ltd. Zhejiang, Hangzhou, 310030, China

*Corresponding author e-mail: zhangmaolin-9901@kmec.org

Abstract: In order to ensure the integrity and confidentiality of power data in the era of big data, it is very important to protect the privacy of smart grid data information. Analyzing electricity big data can obtain electricity consumption habits of electricity users to guide the formulation of power supply plans. This experiment uses an asymmetric encryption algorithm. The encryption and decryption of the asymmetric encryption algorithm use two different keys to fully guarantee the security of the blockchain system. The experiment is based on the blockchain technology in photovoltaic microgrid electricity trading, which belongs to the current type of trading, which is divided into five stages. The service provider is a node of the blockchain system. All smart contracts are encrypted by the private key of both parties in the transaction and the public key of the service provider, which fully guarantees the privacy of users. The experimental data shows that the smart contract is decrypted by the private key and the public key of both parties, so as to obtain the relevant information of the transaction and make the corresponding power dispatch work during the transaction period. The blockchain system solves the security and privacy issues of both parties in the absence of a third-party intermediary. Therefore, the use of blockchain technology can achieve a higher degree of automation for point-to-point power transactions.

Keywords: Blockchain Technology, Power Network Privacy Protection, Asymmetric Encryption Algorithm

1. Introduction

Based on this, the energy sector proposed the concept of energy blockchain, because the business model brought by blockchain provides a good prospect for the future development of other industries [1-2]. Energy blockchain includes a wide range of application scenarios. Broadly speaking, energy blockchain can play a role in measurement and certification methods, market organization, energy finance, and other aspects of various fields such as electricity, power grids, and energy Internet loads;
From a small perspective, energy blockchain technology can change the way people trade electricity. For example, microgrid users can trade electricity through a peer-to-peer transaction model. However, the current blockchain-based power transaction has not yet formed a complete system model, so it is very important to study the power network transaction system based on blockchain technology [3-4].

Ren et al. studied the development of power markets in microgrids with the assistance of energy management systems in microgrids. Taking into account the power generation and load in the microgrids, combining the day-ahead market and real-time market, the goal is to maximize revenue, and the optimization algorithm of the microgrid energy control system is given. Finally, the microgrid experimental platform is used to test the performance and accuracy of the algorithm [5]. Wang et al. proposed that multiple photovoltaic users can form a photovoltaic user group. In the photovoltaic user group, because of the difference in photovoltaic power generation and user power consumption behavior, power sharing can be carried out among photovoltaic users [6].

In the current period, the impact of electricity cost and electricity consumption behavior on air quality, grid stability and resilience, and energy security varies greatly at different times, but users still have little motivation to consider or try to change the time they use electricity [7]. Using blockchain technology, the protocol mechanism behind this encrypted electronic currency bitcoin can replace the average level of operation with precise operations, allowing users at any location to determine their own power source through the tools provided by the company, and also allowing users according to market price signals, it can automatically change its electricity consumption habits, thereby optimizing costs and increasing transparency [8-9]. Starting from the basic characteristics of blockchain, the following analyzes the security of blockchain technology, and further explores the application of blockchain technology in the field of power grid information security [10].

2. Research on privacy protection method of electric power network based on blockchain

2.1 The Role of Blockchain Technology in the Power Grid Industry

The decentralization, openness, intelligence, and sharing of blockchain technology are in line with the concept of the Internet of Energy. It can be used in distributed systems. In these systems, nodes do not need to use data encryption, time stamps, and distributed consensus. And economic incentives to trust each other, and it supports peer-to-peer transactions, coordination and collaboration based on distributed credit. Its application in the Energy Internet effectively supports the open interconnection of multiple energy systems, and supports the extensive and detailed participation of multiple users, including grid-connected renewable energy, long-distance power transmission losses, and at the same time solve the demand side Response and network security issues. However, there are still technical shortcomings. The Energy Internet has not fundamentally changed the problems in the energy field, especially the unique market mechanism and business model of the power industry has not fundamentally changed.

2.2 Key Technologies of Blockchain

(1) Asymmetric encryption algorithm

Encryption algorithms can be divided into symmetric encryption and asymmetric encryption. Compared with symmetric encryption, asymmetric encryption has better security. The two parties communicating using the symmetric encryption algorithm use the same key. If the key is leaked, the entire communication will be cracked; unlike symmetric encryption, the encryption and decryption of asymmetric encryption algorithms use two different keys.

In Bitcoin, a randomly generated private key $k$ is used as the starting point, and the defined generation point $G$ is multiplied on the curve to obtain another point on the curve, which is the corresponding public key $K$, as shown in equation (1).

$$ K = k * G $$

(1)
In the formula: $k$ is the private key, $G$ is the generating point, and $K$ is the public key calculated from the elliptic curve.

2) Distributed consensus algorithm

The blockchain is a distributed data ledger. When all nodes participate in accounting and distributed storage of data, how to make all nodes in the blockchain system reach a consensus on the storage information and ensure that the interests of each node are distributed. The first issue considered by the system. In other words, how to ensure whether a transaction in the system is confirmed and the ownership of the accounting rights in the distributed system.

$$R_i = f(T_1, T_2, ..., T_i)$$
$$\text{storep}(R_i) = \text{true}$$
$$\text{discardp}(R_i) = \text{false}$$

Where: $R_i$ is the calculated result of node $N$ ($N \in \text{Node}$); protocol $p$ is the result verification stage, if the result is recognized by most nodes in the system, node $N_i$ will obtain the accounting right of this stage and record the data Verification passed. In the process of each block generation, the protocol $p$ will only verify one $R_i$.

2.3 Security Evaluation of Grid Blockchain

Smart meters are inherently unsafe in design. As billions of connected energy-consuming devices are expected to be connected to the power grid in the next ten years, the power grid is at risk under cyber attacks, but blockchain technology also has natural cyber threat defense capabilities, thanks to the following features of blockchain technology:

1) Prevent data tampering: After the correct application of blockchain technology, all calculations are performed in the form of hashing, and the data is tamper-proof when generated, thereby avoiding the risk of tampering during transmission.

2) Complete data availability: Blockchain technology can store data in a distributed format across multiple nodes. Even if some nodes or servers are compromised, this architecture allows users to retrieve the complete data set.

3) Redundancy: There is no central point of failure in the operation of the blockchain, so this architecture is inherently highly reliable through redundancy.

4) Privacy and control: Blockchain users can choose which data is permanently transparent and which is encrypted, so that only designated recipients can view the data content.

5) Outsourcing calculation: The encrypted data can be sent to a third party for processing, and the data content will not be displayed during this process.

With the improvement of data levels and the decentralization of energy systems, the demand for reliable defense against cyber attacks is growing significantly. Through the correct application of blockchain technology, network and data communication loopholes can be repaired, data confidentiality and privacy can be improved, and various internal and external threats can be effectively prevented. In terms of remedying data communication vulnerabilities, blockchain technology can integrate the pricing and payment functions of the electricity wholesale market into a secure blockchain system, thereby greatly reducing the risk of incorrect data injection or price manipulation. It can ensure that a given data set or communication sequence between transaction parties is unchanged. At the same time, blockchain technology can improve the confidentiality and privacy of data.

3. Blockchain-based power network privacy protection method experiment

3.1 Experimental Environment

In order to verify the reliability of the data mining and privacy protection methods proposed in this
paper, simulation examples are used to verify their performance. The experimental environment is shown in Table 1.

### Table 1. Experimental environment

|                |          |
|----------------|----------|
| CPU            | Core i5, 3.1GHz |
| RAM            | 8G       |
| operating system | Windows 10 |
| Development language | Python 3.7 |
| Development environment | Anaconda2 |

3.2 Experimental Procedure

The photovoltaic microgrid electricity transaction based on blockchain technology belongs to the current transaction type, which can be divided into five stages: the internal electricity price determination stage of the microgrid, the user transaction matching stage, the smart contract installation stage, the transaction execution stage, and the transaction settlement. At the stage, the specific transaction process is as follows.

1. **The internal electricity price determination stage of the microgrid**
   - From 120 minutes before the time before the transaction to 100 minutes before the time before the transaction is the stage of determining the internal electricity price of the microgrid, the determination of the internal electricity price of the microgrid is completed by the power purchase user group with the assistance of the service provider. According to the relationship between the total purchased power and the total received power in the microgrid, and each user can obtain the internal power transaction volume of the microgrid.

2. **User transaction matching stage**
   - 90 minutes before the current transaction to 20 minutes before the current transaction is the user transaction matching stage. Each user can freely sign smart contracts for related transactions based on the internal electricity price in (1) and the transaction volume obtained.

3. **Smart contract installation stage**
   - Smart contracts need to be installed on the blockchain to function. Smart contracts for related transactions are not installed on the blockchain immediately after signing. Smart contracts are installed before the transaction starts 20 minutes before the current time. Once the external environment changes significantly, smart contracts are not installed, and real-time trading markets are used as remedial measures.

4. **Transaction execution stage**
   - During the trading period of the transaction immediately before the transaction execution stage, the service provider reads the smart contract transaction content to complete the scheduling task, and the user energy management system assists in controlling the user's electricity consumption behavior based on the smart contract content.

5. **Transaction settlement stage**
   - After the trading period is over, the settlement of each user's transaction is completed according to the forecast error compensation settlement model, and the transfer of transaction funds is completed by a smart contract.

4. Discussion on privacy protection methods of power network based on blockchain

   (1) After the internal electricity price of the microgrid is determined in each trading period, based on the blockchain technology, each user will perform random matching transactions based on the transaction volume obtained in the microgrid, which can ensure the privacy of user transactions. Confirm that the two parties of the transaction sign the smart contract of the transaction. Taking the trading time 17:00 as an example, two users are selected. After the internal electricity price of the microgrid is determined, user 1 and user 2 reach a transaction agreement and sign a smart contract for...
the transaction during random matching. User 1 purchases 0.266 kW-h of electricity from user 2, and the unit price is 0.90 (yuan/kW-h). The contract also stipulates that the transaction time is 17:00-18:00, and the settlement time of the transaction is 18:00. For the sake of simplicity, suppose the account address of user 1 is 0x01, and the account address of user 2 is 0x02. The data to be recorded by the smart contract of this transaction is shown in Figure 1.

![Figure 1. Information that the smart contract needs to record](image)

(2) The service provider is a node of the blockchain system, because all smart contracts are encrypted by the private key of both parties to the transaction and the public key of the service provider, which fully guarantees the privacy of users. The service provider can decrypt the smart contract with the private key and the public key of both parties, so as to obtain the relevant information of the transaction and make the corresponding power dispatch work during the transaction period. When the transaction time ends, that is, at 18:00, the smart contract will clear the transaction based on the data collected by the blockchain system from the two-way meter and recorded on the blockchain. The transaction is settled according to the prediction error compensation model, and the smart contract automatically executes the fund transfer according to the transaction settlement result. Assuming that there is no default in all transactions during this trading period, the changes in the balance of each account after the end of the transaction are shown in Table 2.

| User     | Account balance increase/decrease/yuan |
|----------|----------------------------------------|
| User 1   | -0.11                                  |
| User 2   | +0.28                                  |
| User 3   | -0.04                                  |
| User 4   | -0.01                                  |
| User 5   | -0.05                                  |
5. Conclusion

In view of the problems of poor information security, high operating costs, and difficulty in ensuring user privacy in the centralized power transaction structure, this paper studies the use of blockchain-based power network privacy protection methods, that is, using the smart technology of blockchain technology in power transactions. The form of contract stores power transaction information and is responsible for the execution of fund transfers. The central agency only conducts safety checks and congestion management on the concluded power transactions. The service provider in this experiment is a node of the blockchain system. All smart contracts are encrypted by the private key of both parties to the transaction and the public key of the service provider, which fully guarantees the privacy of users.

References

[1] Ren Y, Leng Y, Zhu F, et al. Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network[J]. Sensors, 2019, 19(10):2395-.
[2] Wang D, Zhao J, Wang Y. A Survey on Privacy Protection of Blockchain: the Technology and Application[J]. IEEE Access, 2020, PP(99):1-1.
[3] An J, Yang H, Gui X, et al. TCNS: Node Selection With Privacy Protection in Crowdsensing Based on Twice Consensuses of Blockchain[J]. Network and Service Management, IEEE Transactions on, 2019, 16(3):1255-1267.
[4] Jia B, Zhou T, Li W, et al. A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks[J]. Sensors, 2018, 18(11):3894-.
[5] Fan K, Ren Y, Wang Y, et al. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G[J]. IET Communications, 2018, 12(5):527-532.
[6] Chen B, Wu L, Wang H, et al. A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6):5813-5825.
[7] Kim KJ, Hong SP. Study on Rule-based Data Protection System Using Blockchain in P2P Distributed Networks[J]. International Journal of Security and its Applications, 2016, 10(11):201-210.
[8] Shen M, Deng Y, Zhu L, et al. Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach[J]. IEEE Network, 2019, 33(5):27-33.
[9] Yang C, Tan L, Shi N, et al. AuthPrivacyChain: A Blockchain-based Access Control Framework with Privacy Protection in Cloud[J]. IEEE Access, 2020, PP(99):1-1.
[10] Mohammadinejad H, Mohammadhoseini F. Privacy Protection in Smart Cities by a Personal Data Management Protocol in Blockchain[J]. International Journal of Computer Network and Information Security, 2020, 12(3):44-52.