Blockchain Auditing Technology for Inter-provincial Generation Right Trading

Jianhu Lv1*, Lin Zhou2, Shuo Liu2, Shuo Zhang2, Liangqi Si2, Guodong Li2 and Ailin Chen1

1 Electric Power Research Institute (Nanjing), Nanjing, Jiangsu, 210003, China
2 Beijing Power Exchange Center, Beijing, 100031, China
*Corresponding author’s e-mail: lvjianhu@epri.sgcc.com.cn

Abstract. This paper proposed an auditing method for medium and long-term inter-provincial generation right trading based on blockchain technology, ensuring that market participants' private data and trade secrets cannot be tampered, and the transaction process can be traced back. In this way, trading institutions and regulatory authorities can obtain credible data. The method can provide a two-way book to trace the flow of energy and financial assets, provide data verification services to confirm the integrity and validity of the data, and it can provide data auditing service to identify contents that have been tampered. This paper took the generation right trading between the East and the West of China as an example, a blockchain testing environment was established to verify the feasibility of the auditing method for generation right trading. This paper offered an auditing solution for registration, declarations, clearing, and settlement of data involved in inter-provincial generation right trading.

1. Introduction

On October 24th, 2019, the Political Bureau of the CPC Central Committee conducted the eighteenth collective study on the status quo and trends of blockchain technology development. General Secretary Xi Jinping emphasized that the integrated application of blockchain technology plays an important role in new technological innovation and industrial transformation. It is necessary to use the blockchain as an important breakthrough for independent innovation of core technologies, clarify the main direction, increase investment, focus on a number of key core technologies, and accelerate the development of blockchain technology and industrial innovation. Therefore, accelerating the development of blockchain technology will become a national strategy.

In order to meet the needs of the development of the new era, in 2019, the State Grid Corporation of China proposed the "three-type two-network" strategic goal, building a hub-type, platform-type, shared-type strong smart grid and ubiquitous power Internet. The blockchain technology is one of the key application technologies. On August 22th, 2019, State Grid Corporation set up a blockchain company to realize a new model of blockchain + power grid.

Although China's load centers are far away from the energy centers, thanks to the development of the UHV power grid, the eastern load centers can still absorb the clean energy of the central and western regions and achieve sustainable social development, among which the role of generation right trading across provinces cannot be ignored. As an important market-oriented means for the power industry to promote energy conservation and emission reduction and improve resource utilization efficiency, generation right trading has unique advantages compared with the planned economy, and it
also has the necessary and foundation for continuous and extensive development. On the one hand, when power generation shares are transferred from high-energy and high-emission units to low-energy and low-emission units, the total amount of carbon emissions is reduced. On the other hand, when clean energy power generation participates in generation right trading, it can stimulate clean energy power consumption, avoid the phenomenon of abandoning wind and abandoning light on the power transmission end, and it is also beneficial to the environmental protection of the power receiving end. In the first half of 2019, Beijing Power Exchange Center gave priority to special market transactions of generation right trading, vigorously promoted clean energy alternative to conventional energy, and carried out clean energy generation right trading of 1.8 billion kwh[1].

The market participants are equal and mutually beneficial, requiring the safe flow of electricity, data and financial assets. Two-way transaction deposits are necessary. In this respect, blockchain technology has advantages. The blockchain adopts the most advanced information technology such as distributed ledger, security authentication, consensus mechanism, and intelligent contract. It is the underlying implementation technology of digital financial assets. It has the characteristics of decentralization, data untamperable, and self-healing. It is widely used in the field of commodity circulation. In recent years, it has become a hot technology in the electricity market[2-5], energy Internet[6-7], and distributed energy[8-9] transactions. In terms of data deposit, the paper[10] explored the issue of the authenticity of data related to blockchain deposits and introduced its application in judicial review and evidence collection. The paper[11] introduced the application of blockchain auditing in security systems. The paper[12] used blockchain technology for data integrity verification. The paper[13-14] proposed a blockchain auditing method for the government. The paper[15] described the blockchain for renewable energy certificates and carbon emission certificate transactions, tracking the process of power generation to certificate ownership transactions.

According to the demand of inter-provincial generation right trading, this paper uses blockchain technology to write the transaction core secret data into the blockchain account, design a safe and reliable auditing technology for inter-provincial generation right trading to realize the blockchain data auditing service, to ensure that transaction data can not be tampered, and the transaction process can be traced to meet the regulatory requirements of power transactions.

2. Design of blockchain auditing for inter-provincial generation right trading
The blockchain auditing for inter-provincial generation right trading can be composed of multiple provinces’ transaction blockchain auditing network interconnections. The difficulty of the blockchain auditing is the blockchain network structure, access control rules and smart contracts design.

2.1. Design of blockchain auditing network structure
The network structure of blockchain auditing for inter-provincial generation right trading includes organization, network nodes and smart contract deployment. The organizational division is the basis for the design of the network structure of blockchain auditing for inter-provincial generation right trading. The Organizations which audit inter-provincial generation right trading data are divided into trading institutions and regulatory agencies by type. Divide the organization according to Table 1, and name the organization by referring to the domain name of the network.
Table 1. Blockchain auditing data model for inter-provincial generation right trading

| No | Dimension       | Subitem                                                                 |
|----|-----------------|-------------------------------------------------------------------------|
| 1  | Domain          | Region, province                                                        |
| 2  | Organization    | Industry, enterprise, institution, etc.                                 |
| 3  | Trading process | Registration, declaration, clearing, settlement, etc.                   |
| 4  | Market          | Electric generation, electric power generation, seller, consumer, trading institutions, regulatory agencies, etc. |
|    | participants    | Start time, end time, seller, transmission, purchaser, declaration curve, transaction curve, settlement energy, settlement price, settlement of fee, etc. |
| 5  | Trading         | declaration curve, transaction curve, settlement energy, settlement price, settlement of fee, etc. |
|    | information     | Name, alias, description, market role, address, legal                   |
| 6  | participants    | representative, social identification number, phone, email, bank account, country, organization, etc. |

On the basis of the organization, the blockchain network cluster nodes are designed. Cluster nodes include compute node clusters, ledger database clusters, certificate authority clusters, and consensus clusters.

The smart contracts are installed and instantiated on the compute node clusters in trading institution. Smart contracts include five parts: market participants registration, transaction declaration, transaction clearing, transaction settlement and data auditing. The intermediate results of market participants registration, transaction declaration, transaction clearing and transaction settlement are not stored in the account book, only the secret data such as electricity quantity, electricity price and electricity fee are linked. Data auditing only links the digital summary information of market participants registration, transaction declaration, transaction clearing, and transaction settlement.

2.2. Design of blockchain auditing access control rules

Access control rules can realize the access control of different identity users to different types of data on different blockchains, and ensure the security of data access.

The Access control rules includes identity control, channel control and private data access control. Different identity users verify their identities through digital certificates. Different identity users join different channels to access different blockchain ledgers. At the same time, authorized cross chain access rights are configured. The channels include transaction channel and auditing channel. The transaction channel accesses the market participants registration, transaction declaration, transaction clearing, transaction settlement account book, and the auditing channel accesses the auditing account book. The users who join the transaction channel only have limited access to market participants registration, transaction declaration, transaction clearing and transaction settlement data and services that match their identities. The users who join the auditing channel can access the auditing data and services of market participants registration, transaction declaration, transaction clearing and transaction settlement in the auditing account book. The market participants registration, transaction declaration, transaction settlement and transaction settlement contract are designed with private data ledger to ensure the data access security.

2.3. Design of auditing smart contracts

Smart contracts of blockchain auditing include market participants registration, transaction declaration, transaction clearing, transaction settlement and transaction auditing smart contracts.

2.3.1. Market participants registration smart contracts

The smart contracts of market participants registration provide interfaces for writing market participants registration information, reading market participants registration information and cancelling market participants.
• Writing interface accepts JSON structural parameters, including name, alias, description, market role, legal representative, social ID, address, telephone, email, bank account, etc. When the writing interface is called cross chain, the market participants hash is returned.
• Reading interface accepts market participants hash, or telephone, or bank account number, or identification code, or email and other parameters, and returns the market participants registration information.
• Cancelling interface accepts the hash parameter of market participants, deregisters the record of market participants. When the cancelling interface is called cross chain, the result of deregistration is returned.

2.3.2. Transaction declaration smart contracts
The smart contracts of transaction declaration provide interfaces for writing declaration data and reading declaration data.
• Writing interface accepts JSON structured parameters, including market participants hash, transaction type, transaction time, subject matter, declaration data, When the writing interface is called cross chain, the auditing hash is returned.
• Reading interface accepts the hash parameter of the market participants and returns the transaction declaration data matching the identity.

2.3.3. Transaction clearing smart contracts
The smart contracts of transaction clearing provide interfaces for writing clearing data and reading clearing data.
• Writing interface accepts JSON structured parameters, including transaction type, subject matter, power purchaser hash, seller hash, transmission hash, trading period, clearing price, clearing energy, trading energy, etc. When the writing interface is called cross chain, the auditing hash is returned.
• Reading interface accepts JSON structured parameters, including market participants hash, transaction type, subject matter and transaction time, and returns the transaction clearing results matching the identity.

2.3.4. Transaction settlement smart contracts
The smart contracts of transaction settlement provide interfaces for writing settlement data and reading settlement data.
• Writing interface accepts JSON structured parameters, including market participants hash, transaction type, subject matter, power purchaser hash, transmission hash, seller hash, settlement period, settlement electricity quantity, settlement price, settlement expense, etc. When the writing interface is called cross chain, the auditing hash is returned.
• Reading interface accepts the hash parameter of the market participants and returns the transaction settlement results matching the identity.

2.3.5. Transaction auditing smart contracts
The smart contracts of transaction auditing provide interfaces for writing transaction auditing data, verifying transaction, screening data and tracking assets.
• Writing interface accepts JSON structured parameters, including market participants registration, transaction declaration, transaction settlement or transaction settlement, and returns the auditing hash.
• Verifying interface accepts JSON structured parameters, including the hash parameter of the market participants, transaction declaration, transaction settlement, and returns the verification results.
• Screening interface accepts JSON structured parameters, including the hash parameter of the market participants, transaction declaration, clearing or settlement data, and returns the screening results.
• Tracking interface accepts JSON structured parameters, including the hash parameter of the market participants or transaction period, and returns the JSON structured results of assets flow, which include transaction declaration, clearing or settlement of JSON structured data.

3. Verification of blockchain auditing for inter-provincial generation right trading
This paper took the generation right trading between the East and the West of China as an example, as shown in Figure 1. A blockchain testing environment was established to verify the feasibility of the auditing method for generation right trading.

![Figure 1. Organization structure of inter-provincial generation right trading](image)

Based on the above case, the verification environment of blockchain auditing was built using the 1.4.2 release of Hyperledger Fabric. Assume that the organization of the inter-provincial generation right trading is genergy.net, the organization of the blockchain auditing were exchange institutions (exchangeorg) and regulatory agencies (regulatororg). The cluster consisted of 5 computing nodes (peer), 5 ledger database nodes (couchdb), 2 authentication nodes (ca), and 3 sorting nodes (orderer). the consensus mechanism used the raft algorithm. Raft algorithm was used as consensus mechanism. The node configurations are shown in Table 2.

| Category       | Node                                      | Purpose               |
|----------------|-------------------------------------------|-----------------------|
| Computing      | peer0.exchangeorg.genergy.net             | Deploy smart contracts|
|                | peer1.exchangeorg.genergy.net             |                       |
|                | peer2.exchangeorg.genergy.net             |                       |
|                | peer0.regulatororg.genergy.net            | Deploy smart contracts|
|                | peer1.regulatororg.genergy.net            |                       |
|                | couchdb0.exchangeorg.genergy.net          | Deploy ledger database|
|                | couchdb1.exchangeorg.genergy.net          |                       |
|                | couchdb2.exchangeorg.genergy.net          |                       |
| Distributed ledger | couchdb0.regulatororg.genergy.net     | Deploy ledger database|
|                | couchdb1.regulatororg.genergy.net        |                       |
|                | orderer0.genergy.net                      | Consensus ranking     |
|                | orderer1.genergy.net                      |                       |
|                | orderer2.genergy.net                      |                       |
| Ordering       | ca.exchangeorg.genergy.net               | Authentication service|
|                | ca.regulatororg.genergy.net               |                       |

All 3 peer nodes of exchange institutions were installed and instantiated with smart contracts for market participants registration, transaction declaration, transaction clearing and transaction settlement. 2 peer nodes of regulatory agencies were installed with transaction auditing smart contracts, among them, peer 0 node was set as anchor peer, which is used to build distributed network interconnection for computing cluster between institutions. In order to ensure the security of private data of all market participants, the secret data was configured as private data ledgers, which cannot be accessed by other institutions. Each peer node had a separate accounting database node. The sorting node was not divided into exchange institutions and regulatory institutions, which embodies the characteristics of decentralization. Exchange institutions and regulators established their own independent certification
centers, which are responsible for role certification and certificate issuance of blockchain cluster nodes, administrators and users deployed in their own institutions.

5 smart contracts were written in Go, including registration contract (register_cc), declaration contract (bid_cc), clearing contract (clearing_cc), settlement contract (settle_cc), and audit contract (audit_cc). Through the Node.js interface, the test script (service_start.sh) was written to start and initialize the blockchain network, including channel configuration, certificate generation, creation of creation blocks, creation of identity, creation of channels, joining of channels, update of anchor points, and installation of contracts, instantiating contracts. The contracts interface test script (interface_test.sh) was written, including batch writing market participants registration information, batch writing transaction declaration information, batch writing transaction clearing information, batch writing transaction settlement information, auditing verification, auditing screening, auditing trail.

The test results in the local virtual machine environment show that the performance of raft consensus algorithm is greatly improved compared with Kafka algorithm, and the raft consensus algorithm can record 8 audits per second, which is slow in efficiency. But, if the nodes are deployed on the server physical machine, the throughput can be increased from 4000 to 20000 audits per second, meeting the practical requirements. If a test node goes down, it can automatically obtain the historical blocks from other nodes. The nodes have the ability of self-healing, and there is no loss of audit data. If the number of instances is increased, the self-healing ability will be improved, but the consensus efficiency will be reduced. By using Kubernetes or Swarm, the blockchain network can realize autonomy, which meets the requirements of intelligence.

The above test results show that after performance optimization, the blockchain auditing can meet the technical requirements of distributed computing, high concurrency, security, reliability and intelligence, and can provide a solution for inter-provincial generation right trading audit.

4. Conclusion
This paper designs a blockchain auditing network for inter-provincial generation right trading, and writes the transaction core data and its audit into the blockchain ledger, so that the capital flow and energy flow between the market participants cannot be tampered and can be traced back, which has important application value. At present, this paper is only a simple technical verification, which can be extended to other energy industries, such as natural gas. However, different energy industries may have different transaction audit models and organizational structures, which requires targeted research. In order to meet the higher requirements of real-time and concurrency of other types of power transactions between provinces in the future, it is necessary to propose a special consensus algorithm for the transaction rules to further improve the performance.

Acknowledgments
This research was financially supported by Beijing Power Exchange Center.

References
[1] China Power, (2019) Beijing Power Exchange Center released the trading information of electricity market in the first half of 2019. http://www.chinapower.com.cn/dwsj/20190726/1282118.html.
[2] CNKI, (2019) Research on competitive price power transaction based on blockchain technique. https://doi.org/10.19678/j.issn.1000-3428.0054838.
[3] Lu, J., Song, B., Xiang, w., et al. (2017) Smart contract for electricity transaction and charge settlement based on blockchain. Computer Systems & Applications, 26: 43-50.
[4] Ouyang, X., Zhu, X., Ye, L. (2017) Preliminary applications of blockchain technique in large consumers direct power trading. Proceedings of the CSEE, 37: 3737-3745.
[5] Li, B., Cao, W., Qi, B., et al. (2017) Overview of application of block chain technology in ancillary service market. Power System Technology, 41: 736-744.
[6] Tai, X., Sun, H., Guo, Q. (2016) Electricity transactions and congestion management based on blockchain in energy internet. Power System Technology, 40: 3630-3638.

[7] Liu, S., Yan, Y., Ding, Q., et al. (2017) Application of blockchain in energy internet: advantage, scenario and case. Zhejiang Electric Power, 36: 1-4.

[8] CNKI, (2019) Credit risk management in distributed energy resource transactions based on blockchain. https://doi.org/10.13334/j.0258-8013.pcsee.181888.

[9] Alam, A., Islam, M.T., Ferdous, A. (2019) Towards Blockchain-based Electricity Trading System and Cyber Resilient Microgrids. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). Cox'sBazar. pp. 1-5.

[10] Li, J., Li, Z. (2018) Research on authenticity of electronic data stored on blocks based on blockchain. Computer Engineering & Software, 39: 109-112.

[11] Cha, S., Yeh, K. (2018) An ISO/IEC 15408-2 compliant security auditing system with blockchain technology. In: 2018 IEEE Conference on Communications and Network Security (CNS). Beijing. pp. 20-28.

[12] Rosco, K., Adam, B. (2018) Validating data integrity with blockchain. In: 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). Nicosia. pp. 60-66.

[13] Abreu, P.W., Aparicio, M., Costa, C.J. (2018) Blockchain technology in the auditing environment. In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). Caceres. pp. 1-6.

[14] Antipova, T. (2018) Using blockchain technology for government auditing. In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). Caceres. pp. 1-6.

[15] Ashley, M.J., Johnson, M.S. (2018) Establishing a secure, transparent, and autonomous blockchain of custody for renewable energy credits and carbon credits. IEEE Engineering Management Review, 6: 100-102.