Design of online audit mode based on blockchain technology

Zhuo Yu\textsuperscript{1,*}, Yong Yan\textsuperscript{2}, Chao Yang\textsuperscript{3} and Aiqiang Dong\textsuperscript{1}

\textsuperscript{1}Beijing Zhongdian Puhua Information Technology Company, Beijing 100192, China
\textsuperscript{2}State Grid Zhejiang Electric Power Company Electric Power Research Institute, Zhejiang Hangzhou 310009, China
\textsuperscript{3}State Grid Liaoning Electric Power Dalian Power Supply Company, Liaoning Dalian, China

*Corresponding author e-mail: null@bupt.edu.cn

Abstract. In order to solve the problems of resource sharing difficulties, privacy exposure risks, illegal data invocation and cross-system consistency in traditional audit mode, this paper proposes an online audit mode based on block chain. Firstly, the traditional audit process is analyzed and summarized, and then an audit framework based on block chain is designed. On this basis, a process based on Intelligent contract is designed for the audit mode, and an online audit data platform architecture based on alliance chain is proposed. A feasible online audit under block chain environment is proposed. The implementation method helps to solve the existing problems in auditing. The scheme provided in this paper has a certain operability, which promotes the application of block chain in the field of auditing.

1. Introduction
As the national economy continues to develop, the importance of auditing has become increasingly prominent. The traditional post-event audit, static audit, and on-site audit gradually transition to the direction of concurrent auditing, dynamic auditing, and remote auditing, so as to maximize the role of auditing and monitoring. According to the analysis of the malpractice of China's audit, combined with the problems arising from the traditional audit process, the online audit framework based on blockchain technology, online audit mode and online audit data platform technology architecture are proposed from the supervision level.

2. Current audit mode positive drawbacks

2.1. Divided into two parts: traditional on-site audit and real-time audit
The traditional audit mode application is mainly two parts: on-site audit and real-time audit. The analysis of on-site audit mainly refers to the audit mode applied in the government audit department or enterprise internal audit. Specifically, in the audit work, the audit work of related financial documents such as receipts, invoices, details, bills, bank flow, cash amount, payment, etc. are handled uniformly. In general, the main characteristics of on-site audit analysis are: long audit cycle and many auditors. The internal audit of the enterprise is based on the relevant auditing system and the auditing cycle, and the auditing cycle is carried out. The comparative analysis of the government audit focuses on the issue of corporate tax payment. The audit focus of the enterprise is: the application status of the internal funds of the enterprise, and whether there is corruption. Phenomenon, evaluation of the application of funds.
Real-time audits are currently used primarily in government-owned state-owned enterprises, as well as in some private sector audits. Real-time auditing is more efficient than traditional on-site auditing, and auditing accuracy is high. The specific application mainly through computer technology, network technology, software technology, remote control technology to carry out relevant audit data transmission, completed audit operation mode.

2.2. Pattern analysis

Analysis of the traditional on-site audit mode and real-time audit mode, the audit effectiveness of the two audits in the actual application is relatively good, but in the actual application, the focus of the two audit modes, on the field audit and the selection of real-time audit mode, Enterprises should also select and apply corresponding audit technologies according to their own development characteristics and analysis of audit application purposes.

![Diagram of Audit Mode]

Figure 1. Audit mode.
3. Building an audit framework based on blockchain technology

China's auditing industry has developed rapidly, but there are still many problems to be solved. First, the lack of audit data resource sharing; second, it is difficult to guarantee the privacy of information subjects; third, operational risk assessment and audit abnormality warning for data; fourth, cross-system multi-dimensional data is difficult to ensure data consistency.

3.1. Distributed micro-application end-to-end build service to achieve trusted sharing of data resources.

The intelligent contract supported by the blockchain technology supports the implementation of simple application logic and has the ability to build trusted micro-applications in the blockchain environment, providing a new way of constructing and executing the audit business logic. The micro-application built by the blockchain technology realizes the end-to-end execution of the audit data, and the data collected by the micro-service is stored on the blockchain through the approval of the nodes of the whole network. The decentralized distributed storage structure enables auditors to grasp every move of the audited unit's business activities in real time. By utilizing the autonomy of the blockchain technology and the intangible characteristics of the information, the audited entity can be prevented from tampering with the accounting data to ensure the authenticity of the data of the audited entity.

3.2. The privacy service guarantees the privacy of the information subject.

Audit data is related to the business status of the company and the corporate image. In the audit process, the privacy of the audit data subject must be protected. Utilizing the combination of the advanced encryption method of the blockchain technology and the hashing method, the user identity is hash-transformed, the transmission channel is sliced and encrypted, and the personal data is block-
encrypted to realize the user's personal data and operation data. Anonymous security and transport security.

3.3. Trusted services realize auditing abnormal warnings, and then carry out operational risk assessment.
In the aspect of user behavior monitoring, the system-based monitoring method is adopted, and the monitoring of the user's cross-system privilege operation is still not comprehensive enough, and there are problems such as misoperation caused by the privilege update not being timely. Using the trustworthy characteristics of the blockchain technology, the credibility of the data invocation process is realized, and the security of the data invocation process is improved. The use of blockchain technology intelligent contract certification, providing a strict authorization software calling function, reducing illegal calls. The use of the trusted distributed storage feature of the blockchain technology improves the synchronization efficiency when the rights are updated, and avoids misoperations caused by inconsistent permissions.

3.4. Consistent services enable multi-dimensional consistency requirements across system data.
Although various departments have mastered a large amount of business data, because the information between the various agencies is not circulated, the data dimensions of each organization are different, which has caused great obstacles to the audit work. Using the blockchain technology, the overall information and dynamic information of the data dimension are uniformly stored, and the multi-node backup is performed by using the non-tamperable characteristics of the information, and the multi-party comparison verification method is used at the running time to dynamically adjust the consistency of the user's data resources.

4. Blockchain-based auditing model
This paper adopts the framework of alliance chain to build a multi-industry audit data platform based on blockchain. The blockchain-based auditing model is to use the blockchain technology to reshape the existing auditing system and auditing organization system, and to innovate the audit implementation process.

![Blockchain-based audit implementation process](image)

**Figure 3.** Blockchain-based audit implementation process
1) Obtain a public key and a private key by registration, and formulate a smart contract with the audit method and rules, and pass the smart contract signed by the private key into the blockchain network;

   When an audit is required, the user first obtains the public key and the private key through registration. The auditing unit formulates a smart contract with the auditing method and rules, and then signs it with the private key. The signed smart contract is transmitted to the blockchain network.

2) Verifying the validity of smart contracts in the incoming blockchain network through the authoritative node of the audit authority;

   Then, the smart contract in the incoming blockchain is uniformly verified, and the smart contract is spread through the network and stored in each node of the blockchain. Once the consensus mechanism is triggered, the smart contract is verified by the audit effectiveness, when verifying the validity of the contract, it is verified by the authoritative node (master node). Among them, the consensus is that the blockchain adopts a process of identifying and verifying transaction information by a node with consensus authority without having to recognize each other and establish a trust relationship. Only the consensus transaction is completed. It will be written to the block and stored in the blockchain.

3) After the validity verification of the smart contract is successful, the smart contract is integrated into a hash block ID, and the hash block ID is spread to the entire network;

   Once the validity of the smart contract is verified successfully, the smart contract is integrated into a hash block ID and quickly spread to the whole network. After the consensus is consistent, the hash block ID is returned to the platform to determine the legitimacy of the audit method.

4) Monitor whether the auto-execution time written in the smart contract expires or monitor whether the transaction of the smart contract satisfies the execution condition of the parameter requirement;

   Smart contract execution is generally done in two cases, one is the automatic execution time expiration written in the smart contract, and the other is the transaction to the execution condition of the parameter requirements. In the blockchain network, the monitoring node periodically traverses the auto-execution state, transaction, and trigger conditions of each smart contract to determine whether the monitoring smart contract reaches the automatic execution condition.

5) After the smart contract reaches the automatic execution condition, the audit data corresponding to the smart contract is verified in the blockchain network;

   When an intelligent contract reaches the condition of automatic execution, the audit data corresponding to the intelligent contract is read from the block chain, and the consistency verification is carried out in the block chain network. That is to say, the consensus of audit data is carried out again, which proves that the audit data has not been tampered with.

6) When the audit data consistency verification corresponding to the smart contract is passed, the entire transaction and state processing of the smart contract is automatically completed.

   When the audit data consistency verification corresponding to the smart contract passes, that is, after the double consistency verification is completed, the smart contract automatically completes the processing of the entire transaction and state. Dual consistency verification ensures that this process is transparent and not tamperable.

5. Technical architecture of online audit data platform

For the online audit data platform, in the overall architecture of the platform, it is mainly composed of seven layers: application layer, contract layer, consensus layer, network layer, data layer, data security
sharing mechanism layer and trusted access layer of terminal equipment. The technical architecture of
the online audit data platform is shown in the figure.

![Figure 4. technical architecture of the audit data platform](image)

Application layer: the application layer is oriented to the application scenario of audit data, providing corresponding information flow for audit data supplier, audit data demander and supervision institution. Through the interaction with the application layer, the supplier of audit data and the demander of audit data can interact with audit data efficiently. Audit information subjects can trace authorization records to ensure the security of their own information.

Contract layer: the contract layer includes contract template construction, contract resolution and instantiation, contract publishing, contract configuration, and so on. In order to effectively blockchain data intelligent contract standardization, implementation according to user requirements, formulate contract text, was carried out on the contract text formalization, and choosing the appropriate modeling language and modeling tools to nature of modeling and validation rules of formal documentation, can make all kinds of contracts to ensure appropriate transaction, in the case of without external factors interference efficiently.

Consensus layer: the consensus layer encapsulates the consensus mechanism of the whole system. Consensus mechanism includes consensus algorithm and blockchain monitoring and management related functions. The consensus algorithm of this system adopts Byzantine algorithm. Blockchain monitoring and management requires the monitoring of blockchain status and the management of blockchain network to improve the processing performance of blockchain. In addition, through blockchain monitoring, the pre-block size, data update time and the amount of data written to block are set to improve the performance of block data storage.

Network layer: the network layer encapsulates the network protocol, node management, network configuration and other elements of the platform. Node management ensures that regulators can understand the running state of each node. The network configuration management mechanism ensures that the nodes in the platform can connect to each other stably and trade audit data.

Data layer: each node in the platform can load the transaction data generated in a certain period into the data block and link to the previous block according to the specific Merkel tree and Hash algorithm. In this process, it mainly involves Hash algorithm, timestamp, chain structure and Merkle tree.

Data security sharing mechanism layer: there is a large amount of data stored in the system, which needs to ensure the security of data content and data forwarding process. Therefore, it is necessary to
study the data content management, data forwarding and encryption mechanisms. Data security sharing mechanism layer mainly includes centralized data naming technology and service, authorized data distributed storage and traceability, and data encryption and adaptation.

Trusted access layer for terminal devices: there are various terminal devices with different interfaces. The trusted access layer for terminal devices facilitates quick and trusted access for different types of terminal devices. It mainly includes protocol analysis, authentication, consistency judgment and switching management.

6. Conclusion
This paper introduces the online audit framework, online audit mode and the technical framework of online audit data platform based on blockchain technology, and puts forward a practical and feasible online audit implementation method under the blockchain environment, which is helpful to solve the existing problems of audit. The audit method based on blockchain is decentralized and subversibly changes the current audit mode. Since the research and basic theories of blockchain technology have not been fully mature, the application in various fields is still being explored step by step. This paper hopes to provide a way of thinking for the application of blockchain technology in the audit industry and provide reference for future research.

Acknowledgement
This work is funded by the State Grid Corporation of Science and Technology Project (52110417000G).

References
[1] Huang Guanhua. Research on improved network audit method of block chain[J]. Financial Science, 2016(10):84-91.
[2] Zhang Fengyuan, Wu Shuqi, Ye Chenyun. Opportunities and challenges of audit under blockchain technology[J]. Friends of Accountants, 2018(03):153-155.
[3] Xv Jinye, Zhu Yangyang. Research on the impact of block chain information technology on accounting supervision[J]. Friends of Accountants, 2018(01):156-160.