Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Research on the Security Issues of Engineering Audit Based on Blockchain

Haibo Yi, Tao Qu, Rui Huang, Ningbo Li,Weiping Deng
School of Artificial Intelligence, Shenzhen Polytechnic University, Shenzhen, China
Guangzhou Urban Blockchain Industry Association, Guangzhou, China
WeBank, Shenzhen, China

***Abstract*—The application prospect of the blockchain engineering audit model is broad, thanks to the decentralization, tamper-proof, transparency and security characteristics of blockchain technology itself. This article focuses on the following goals: first, improving the credibility and security of audit data; Second, improve audit efficiency and automation level;**

Third, optimize the audit supervision system; Fourth, promote industry innovation and intelligent development; Propose solutions to address challenges faced in practical applications, and provide a theoretical basis for promoting the widespread application and in-depth development of blockchain technology in the audit industry.

***Keywords* – blockchain，Audit，Engineering，Security**

1.INTRODUCTION

With the rapid advancement of new-generation information technology worldwide, cutting-edge technologies such as big data, cloud computing, artificial intelligence, and blockchain are penetrating into all walks of life at an unprecedented speed, profoundly changing the way of production and life. In the field of construction engineering, this change is particularly significant. The construction engineering information platform is gradually transforming from a traditional information management tool into a strategic hub for enterprises to manage complex and large engineering data. This transformation not only greatly improves the efficiency of data processing and analysis, but also provides more accurate and real-time data support for enterprise decision-making.

Blockchain technology, with its unique features of data encryption, decentralized storage, and tamper-proofing, has built a security barrier for the construction project information platform. It ensures the integrity and credibility of engineering data during transmission and storage, effectively preventing the risk of data being illegally tampered with or leaked, and safeguarding the security of enterprise data assets.

Compared to traditional engineering management models, blockchain-based engineering management models exhibit significant advantages. It can seamlessly integrate all aspects of project management, from initial project application and approval, to mid-term transaction execution and financial processing, to later-stage accounting reports and data analysis, achieving synchronous management of information flow, capital flow, and logistics throughout the entire life cycle. In this process, the functions of instant archiving, efficient storage, accurate accounting and convenient access of information greatly simplify the management process, reduce human errors and improve work efficiency. At the same time, it has completely freed itself from the constraints of paper-based operations, propelling engineering management towards a more standardized, automated, and automated direction.

In addition, the application of blockchain technology also gives enterprises the ability to deeply analyze engineering financial and tax indicators. Through advanced technologies such as smart contracts and data analysis, enterprises can grasp the financial status, tax compliance, and potential risk points of engineering projects in real time, providing strong data support and intelligent assistance for the precise formulation of business strategies, the scientific optimization of investment decisions, the establishment and improvement of risk warning mechanisms, the refined implementation of cost control, and the automated processing of tax compliance checks.

In the field of engineering audit, the application of blockchain also triggers profound changes in the industry. Auditing institutions actively respond to the trend of the times, using the advantages of blockchain technology to conduct comprehensive and in-depth audit supervision of corporate assets, liabilities, and operating results. This process not only ensures the objectivity, fairness, and accuracy of audit results, but also greatly improves the timeliness and transparency of audit reports, providing more authoritative and professional financial evaluation and advice for audited enterprises.

However, it is worth noting that although engineering blockchain auditing has shown great potential and advantages in improving audit efficiency and transparency, it still faces many challenges and tests in practical applications. How to use digital technology more effectively to monitor customer fund flows, ensure comprehensive coverage of audit activities on the authenticity, reliability, and effectiveness of business activities, and address potential issues such as technical complexity and data privacy protection are key topics that need to be focused on and resolved in the current and future periods. Only by continuously overcoming these challenges and fully leveraging the advantages and value of blockchain technology can we promote the development of the construction engineering audit industry towards a more efficient, intelligent, and secure direction.

1.1 Data Integrity

Enterprise users generally store engineering big data on public or private clouds, and data security relies on cloud service providers. When auditing personnel extract engineering data from the cloud, it is an urgent problem to identify whether the integrity of the cloud data has been damaged.

1.2 Authenticity of Data

Compared with the traditional paper-based accounting method, electronic accounting data is more easily tampered with and difficult to leave traces after tampering. It is difficult for audit personnel to judge whether the data on the cloud is authentic or tampered with.

1.3 Data Security

With the widespread application of cloud computing technology, more and more enterprise systems are moving to the cloud. A large amount of enterprise business data is stored on the cloud, which also leads to frequent security incidents on the cloud. Cloud security issues have attracted widespread attention and concern. Engineering data is the core data of an enterprise, and the security of storing it on the cloud is also a key issue that needs to be addressed.

As a key technology of WEB3.0 and the metaverse, blockchain provides a new decentralized data management method. Data stored on the blockchain is tamper-resistant and traceable, offering new insights for engineering integrity audits. Therefore, it is of great value and practical significance to study the blockchain-based engineering audit scheme.

2.RELATED WORK

Blockchain was first used as the underlying technology for digital currencies such as Bitcoin, and has become known to the public as its application in the financial sector has grown. Blockchain has gradually moved away from its single financial attribute and begun to increase its application in logistics, supply chain, intellectual property, healthcare, education and other fields due to its cryptographic underlying infrastructure, decentralized architecture, data on-chain that is not easily tampered with, easy to trace historical records, and support for smart contracts. In 2021, blockchain was listed as a key industry of the national digital economy in the 14th Five-Year Plan, and its future development prospects have attracted more attention. In the local area, the Shenzhen Municipal Government issued a document in May 2022 to promote blockchain as a key industry for Shenzhen's development in the next 5-10 years. Products such as FISCO-BCOS and Changan Chain developed by Tencent, Huawei, WeBank, Ping An Technology and other companies have become representative products of domestic self-controlled blockchain. Among them, FSICO-BCOS has taken a leading position in the blockchain field as a blockchain financial product.

With the vigorous rise of the domestic blockchain industry, the continuous emergence of blockchain technologies and products has laid a solid foundation for research in the field of blockchain auditing. Against this backdrop, pioneering scholars such as Cui Chun have been committed to addressing challenges at the level of basic audit theory [1-5]. In addition, scholars such as Jiang Yaoming, Yang Jiayi, and Tang Yanjun have turned their attention to the deep integration of blockchain technology and national auditing, emphasizing its great potential in breaking data silos, promoting anti-corruption collaboration, enhancing information transparency, exposing hidden corruption, and strengthening audit accountability, injecting new vitality and efficiency into big data anti-corruption [6]. In summary, the extensive and in-depth research on blockchain auditing both domestically and internationally has amply demonstrated that blockchain has become a pivotal technology and future trend in advancing intelligent and digital auditing.

Data integrity audit, as the core part of the engineering big data audit system, is of great importance. Traditional methods rely on digital signatures or MAC message authentication codes, primarily focusing on data verification within the user's local storage environment. The process involves the user first calculating the hash value of the data to be uploaded and storing it locally. Subsequently, the data is uploaded to the cloud service provider. When verification is required, the data is downloaded from the cloud and the hash value is recalculated for comparison, thereby confirming the integrity of the cloud data. However, when dealing with large-scale data, this method faces challenges in terms of economic efficiency and ease of operation due to high communication costs and significant consumption of computing resources.

To address the above challenges, researchers have actively explored the optimization path of data integrity verification mechanisms, with two major mainstream directions particularly compelling: data recoverability proof POR and data possession proof PDP. Especially, PDP technology, by introducing RSA signature to construct homomorphic verification tags, has achieved efficient integrity auditing of cloud storage data, and has become one of the key technologies in the field of digital auditing.

In recent years, innovations around PDP technology have emerged one after another. Wang et al. first proposed a data ownership proof mechanism for public clouds [7], and then explored a distributed PDP mechanism for identity in a multi-cloud environment [8]. Scholars such as Wang, Wu, and Qin further refined the PDP strategy that combines online and offline [9], while scholars such as He, Chen, and Yuan focused on the design of PDP mechanisms in dynamic group environments in the cloud [10]. In addition, scholars such as Wang, He, Fu, etc. proposed a PDP scheme based on outsourcing data transmission optimization [11], and Wang et al. even integrated blockchain technology into the PDP mechanism [12], opening up a new research perspective. Ni, Zhang, Yu and other scholars have constructed an identity authentication cloud storage PDP mechanism through RSA signatures [13], while Li, Wang, He and other scholars have proposed a synchronous PDP blockchain mechanism for digital twin scenarios [14]. Yang, Chen and others have focused on streamlining the optimization of identity PDP mechanisms in cloud storage environments [15].

Based on the above research and more relevant literature [16-22], it can be clearly seen that blockchain audit technology based on PDP is gradually becoming an important force in promoting the development of the audit field, and it has shown great application potential and broad prospects in scenarios such as engineering big data verification.

3. BLOCKCHAIN-BASED ENGINEERING AUDIT SCHEME

3.1 A blockchain-based engineering audit framework

The blockchain-based engineering audit framework mainly consists of the following core components: blockchain underlying platform, data management layer, audit application layer, user access layer, and supervision and compliance layer.

3.1.1Blockchain underlying platform

Selection of blockchain technology: Select the appropriate blockchain technology based on the specific needs and security requirements of the audit project.

Node settings: Set up nodes in the blockchain network, including accounting nodes, verification nodes, etc., to ensure distributed storage and verification of data.

Consensus mechanism: Adopt appropriate consensus mechanisms such as PoW, PoS, DPoS, etc. to ensure that nodes in the network can reach consensus and ensure data consistency and security.

3.1.2 Data management layer

Data collection and preprocessing: Collect various engineering-related data such as contract documents, construction drawings, progress reports, cost data, etc., and perform preprocessing to ensure data consistency and availability.

Data encryption and storage: Utilizing the encryption technology of blockchain, sensitive data is encrypted and stored in the blockchain network, achieving data tamper-proof and traceability.

Data sharing and exchange: Through the technology of smart contract of blockchain, data sharing and exchange between different audit subjects can be realized, and the collaborative efficiency of audit work can be improved.

3.1.3Audit application layer

Audit model and algorithm: Develop models and algorithms suitable for engineering audits, such as risk assessment models and anomaly detection algorithms, to conduct in-depth analysis and mining of data in blockchain networks.

Audit task management: Through the blockchain platform, the whole process management of audit task allocation, progress tracking, and result feedback can be realized, improving the standardization and efficiency of audit work.

Audit report generation: Based on the audit results, an audit report is automatically generated and stored in the blockchain network to ensure the authenticity and traceability of the report.

3.1.4User access layer

Identity authentication and authorization: Through blockchain identity authentication technology, it is ensured that only authorized users can access the audit system.

User interaction interface: Provides a friendly user interaction interface for users to submit, query, and view reports for audit tasks.

3.1.5Regulatory and compliance layer

Compliance: Ensure that the audit system complies with relevant laws and regulations, such as data protection regulations and audit standards.

Regulatory interface: Provide necessary interfaces and tools for regulatory agencies to conduct supervision and review of audit systems.

3.2 Audit data security model and identity authentication model based on lattice cryptography

Engineering data belongs to the core data of an enterprise and needs to be protected. General data can be encrypted using cryptographic algorithms such as AES, RSA, and elliptic curves, and decrypted when needed. Only users with the key or private key can correctly decrypt the encrypted data, which ensures the security of the engineering data. However, with the continuous development of quantum computing technology, it has been theoretically proven that public key cryptographic algorithms such as RSA and elliptic curve can be cracked based on quantum algorithms, and the security of symmetric cryptographic algorithms such as AES can be reduced, which will pose a potential huge threat. Therefore, we should design an audit data security model and identity authentication model that can resist quantum computer attacks, based on post-quantum cryptography represented by lattice public key cryptography, to maintain the underlying security of blockchain auditing.

3.2.1 Audit data security model based on lattice cryptography

3.2.1.1 Model Overview

The audit data security model based on lattice cryptography aims to leverage the intractability of lattice cryptography, such as LWE and SIS, to construct a secure data audit mechanism. This model ensures the security of data during transmission and storage by encrypting the stored audit data, while providing effective data integrity verification and access control functions.

3.2.1.2 Core Components

Data encryption: Utilize lattice cryptography algorithms to encrypt audit data, ensuring the confidentiality of data during storage and transmission. The encryption process may involve steps such as key generation, encryption operations, and decryption operations.

Integrity verification: Verifying the integrity of audit data through digital signatures, hash functions, and other technical means. When data is modified or tampered with, it can be detected and alarmed in a timely manner.

Access control: Based on lattice cryptography, an identity authentication mechanism strictly controls access rights to audit data. Only authorized users can access and modify audit data.

3.2.1.3 Safety features

Quantum-resistant: lattice cryptography is considered to be resistant to quantum computer attacks, so the audit data security model based on lattice cryptography has long-term security guarantees.

Efficiency: With the continuous optimization and improvement of lattice cryptography algorithms, the performance of lattice cryptography-based audit data security models is gradually approaching or even surpassing traditional cryptography algorithms.

Flexibility: The lattice cryptography algorithm supports multiple parameter configurations and variants, allowing for flexible adjustments based on specific application scenarios and security requirements.

3.2.2 Identity authentication model based on lattice cryptography

3.2.2.1 Overview of the model

The identity authentication model based on lattice cryptography utilizes the intractability of lattice cryptography to construct a secure identity authentication mechanism. This model confirms the identity of the user by verifying their identity information such as username, password, biometric features, and authorizes the user to access corresponding resources or services.

3.2.2.2 Core components

Identity identification: assigning unique identity identifiers such as IDs and public keys to each user for identifying the user's identity during identity authentication.

Authentication protocol: Design an authentication protocol based on lattice cryptography to ensure the secure transmission and verification of user identity information. The authentication protocol may involve steps such as key exchange and signature verification.

Key management: Securely manage and store user keys to ensure confidentiality, integrity, and availability of the keys. Key management may involve steps such as key generation, distribution, update, and revocation.

3.2.2.3 Safety features

High security: The identity authentication model based on lattice cryptography utilizes the intractability of lattice cryptography to ensure the security of user identity information, maintaining high security even in the face of powerful attack methods.

Lightweight: Compared with traditional cryptography-based identity authentication models, lattice-based identity authentication models may have advantages in terms of computational complexity and resource consumption, making them suitable for resource-constrained environments.

Scalability: The identity authentication model based on lattice cryptography supports multiple identity authentication methods and scenarios, and can be extended and customized according to specific application requirements.

3.3 Three lattice-based algorithms and models for blockchain data integrity audit

In order to solve the problem that the third party is not trusted in the audit of engineering big data, and the cloud service provider and the user cannot arbitrate when there is a dispute over the integrity of the data, this paper introduces blockchain based on lattice cryptography and proposes a data integrity audit algorithm and model.

3.3.1 Overview of algorithm

The lattice-based blockchain data integrity audit algorithm aims to encrypt, sign, and verify data on the blockchain through the technical means of lattice cryptography to ensure data integrity, authenticity, and tamper-proofness. This algorithm combines the decentralization and tamper-proof characteristics of blockchain with the security advantages of lattice cryptography, providing strong support for data auditing.

3.3.2 Core components

Data encryption: Utilize lattice cryptography algorithms to encrypt sensitive data on the blockchain, ensuring confidentiality during storage and transmission. The encryption process may involve steps such as key generation, encryption operations, and decryption operations, with key management being a critical aspect.

Data signature: Digital signature of data on the blockchain to verify the integrity and authenticity of the data. Digital signatures are generated based on the intractability of lattice cryptography, and are resistant to forgery and denial of service.

Integrity verification: Design a lattice-based integrity verification protocol that allows auditors to confirm the integrity of data by verifying data signatures and hash values. The verification process may involve challenge-response mechanisms, zero-knowledge proofs, and other technical means.

Blockchain technology: Utilize the decentralized and tamper-proof characteristics of blockchain to record transaction history and audit records of data. Each block on the blockchain contains a certain number of transaction records, and is connected to the previous block through a hash pointer, forming an immutable data chain.

3.3.3 Model construction

System architecture: The lattice-based blockchain data integrity audit model usually includes a hierarchical structure of data layer, network layer, consensus layer, contract layer, and application layer. The data layer is responsible for data encryption, signature, and storage; The network layer is responsible for data transmission and communication; The consensus layer is responsible for the consensus mechanism of the blockchain network; The contract layer is responsible for the execution and management of smart contracts; The application layer provides data audit services to users. Audit process: Users upload data to the blockchain network, and encrypt and sign the data. Nodes in the blockchain network record data on the blockchain through a consensus mechanism and generate corresponding transaction records and audit records. The auditor accesses the blockchain network to obtain the data blocks that need to be audited and verifies the integrity and authenticity of the data. If the data is found to be tampered or corrupted, the auditor can initiate an alert or take appropriate remedial measures.

3.3.4 Safety Features

Quantum-resistant: lattice cryptography is considered to be resistant to quantum computer attacks, so the data integrity audit algorithm based on lattice for blockchain has long-term security guarantees.

Efficiency: With the continuous optimization and improvement of lattice cryptography algorithms, the performance of lattice-based blockchain data integrity verification algorithms is gradually approaching or even surpassing traditional cryptography algorithms.

Privacy protection: Through encryption and signature technology, users' private information can be protected from being leaked to unauthorized third parties.

Transparency: The open and transparent nature of blockchain allows all participants to view transaction records and audit records on the blockchain, enhancing the credibility and fairness of the system.

4.CONCLUSION

The application prospect of the blockchain engineering audit model is broad, thanks to the decentralization, immutability, transparency, and security characteristics of blockchain technology itself. First, improve the credibility and security of audit data; Second, improve audit efficiency and automation level; Third, optimize the audit supervision system; Fourth, promote industry innovation and intelligent development. However, there are still some challenges in the practical application process, such as technical costs and difficulties, and imperfections in laws and regulations. To overcome these challenges, it is necessary to continuously strengthen technological research and development and talent cultivation, improve relevant laws, regulations, and standard systems, and promote the widespread application and in-depth development of blockchain technology in the audit industry.

ACKNOWLEDGEMENTS

The authors acknowledge National Natural Science Foundation of China (No. 62202316), Characteristic Innovation Projects in Guangdong Provincial Universities (No. 2022KTSCX308), Scientific Research Startup Fund for Shenzhen High-Caliber Personnel of Shenzhen Polytechnic (No.6021310026K), Key scientific research project of Shenzhen Audit Bureau (No. 24SZSJZC012).

REFERENCES

[1] Kang L , Yang L , Shiyi T ,et al.CFAuditChain: Audit BlockChain Based on Cuckoo Filter[J].The Computer Journal, 2024(6):6.DOI:10.1093/comjnl/bxad133.

[2] Liu S , Yao Y , Tian G ,et al.A blockchain-based compact audit-enabled deduplication in decentralized storage[J].Computer Standards & Interfaces, 2023, 85:103718-.DOI:10.1016/j.csi.2022.103718.

[3] Pratiwi L L .Implementasi Blockchain Pada Akuntansi dan Audit di Indonesia[J].Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan, 2022.DOI:10.32670/fairvalue.v5i01.873.

[4] Anis A , Elkhosht M O .Blockchain in accounting and auditing: unveiling challenges and unleashing opportunities for digital transformation in Egypt[J]. 2023.

[5] Pizzi S , Caputo A , Venturelli A ,et al.Embedding and managing blockchain in sustainability reporting: a practical framework[J].Sustainability Accounting, Management and Policy Journal, 2022, 13(3):545-567.DOI:10.1108/SAMPJ-07-2021-0288.

[6] Parmoodeh A M , Ndiweni E , Barghathi Y .An exploratory study of the perceptions of auditors on the impact on Blockchain technology in the United Arab Emirates[J].International Journal of Auditing, 2022.DOI:10.1111/ijau.12299.

[7] H. Wang, "Proxy Provable Data Possession in Public Clouds," in IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551-559, Oct.-Dec. 2013.

[8] H. Wang, "Identity-Based Distributed Provable Data Possession in Multicloud Storage," in IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328-340, March-April 2015.

[9] Y. Wang, Q. Wu, B. Qin, S. Tang and W. Susilo, "Online/Offline Provable Data Possession," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1182-1194, May 2017.

[10]K. He, J. Chen, Q. Yuan, S. Ji, D. He and R. Du, "Dynamic Group-Oriented Provable Data Possession in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1394-1408, 1 May-June 2021.

[11]H. Wang, D. He, A. Fu, Q. Li and Q. Wang, "Provable Data Possession with Outsourced Data Transfer," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 1929-1939, 1 Nov.-Dec. 2021.

[12]H. Wang, Q. Wang and D. He, "Blockchain-Based Private Provable Data Possession," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2379-2389, 1 Sept.-Oct. 2021.

[13]J. Ni, K. Zhang, Y. Yu and T. Yang, "Identity-Based Provable Data Possession From RSA Assumption for Secure Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1753-1769, 1 May-June 2022.

[14]T. Li, H. Wang, D. He and J. Yu, "Synchronized Provable Data Possession Based on Blockchain for Digital Twin," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 472-485, 2022.

[15]Y. Yang, Y. Chen, F. Chen and J. Chen, "An Efficient Identity-Based Provable Data Possession Protocol With Compressed Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1359-1371, 2022.

[16]H. Wang and Y. Zhang, "On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 264-267, Jan. 2014.

[17]H. Wang, D. He, J. Yu and Z. Wang, "Incentive and Unconditionally Anonymous Identity-Based Public Provable Data Possession," in IEEE Transactions on Services Computing, vol. 12, no. 5, pp. 824-835, 1 Sept.-Oct. 2019.

[18]S. K. Nayak and S. Tripathy, "SEPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage," in IEEE Transactions on Services Computing, vol. 14, no. 3, pp. 876-888, 1 May-June 2021.

[19]J. Li, H. Yan and Y. Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 356-365, 1 Jan.-March 2022.

[20]Y. Zhu, H. Hu, G. -J. Ahn and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[21]D. He, N. Kumar, S. Zeadally and H. Wang, "Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems," in IEEE Transactions on Industrial Informatics, vol. 14, no. 3, pp. 1232-1241, March 2018.

[22]Y. Li, Y. Yu, R. Chen, X. Du and M. Guizani, "IntegrityChain: Provable Data Possession for Decentralized Storage," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1205-1217, June 2020.