Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 3 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i03.53947

PAPER

Development and Evaluation of a Blockchain-Based Financial Audit Tracking System for Mobile Platforms

Eying Liu(✉)

Accounting Department of Business School, Hunan International Economics University, Changsha, China

wuyueyuhan@163.com

ABSTRACT

With the rapid development of blockchain technology, its applications in finance, supply chains, and auditing have garnered widespread attention. Traditional financial auditing faces challenges such as data tampering, audit opacity, and difficulties in traceability, necessitating the development of more efficient, secure, and transparent auditing methods. Blockchain technology, with its decentralized, tamper-resistant, and fully traceable characteristics, has emerged as a powerful tool for addressing the challenges inherent in traditional auditing practices. Especially in the context of the growing prevalence of mobile platforms, the integration of blockchain technology with financial audit tracking systems can not only enhance transparency throughout the auditing process but also significantly improve audit efficiency. However, existing research has primarily focused on the basic applications of blockchain technology, with limited analysis of mobile platform requirements and comprehensive integration of blockchain with audit information tracking mechanisms. In response to this gap, a blockchain-based financial audit tracking system was proposed and developed, comprising two core elements: firstly, a layered structure for the blockchain system that is tailored for mobile platforms, ensuring both security and efficiency; secondly, the implementation of a tracking mechanism for financial audit data, enabling transparent tracking and validation of the entire auditing process via blockchain technology. The results indicate that the system effectively addresses issues such as information tampering, data loss, and audit opacity in traditional financial auditing, providing a safer, more transparent, and efficient solution for financial audits.

KEYWORDS

blockchain technology, financial auditing, information tracking, mobile platforms, system design

1 INTRODUCTION

With the rapid development of information technology, traditional financial auditing methods face numerous challenges, including data tampering, opacity in the audit process, and low audit efficiency [1, 2]. The introduction of blockchain

Liu, E. (2025). Development and Evaluation of a Blockchain-Based Financial Audit Tracking System for Mobile Platforms. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(3), pp. 73–86. https://doi.org/10.3991/ijim.v19i03.53947

Article submitted 2024-08-07. Revision uploaded 2024-11-19. Final acceptance 2024-12-11.

technology offers a novel approach to addressing these issues. Blockchain possesses decentralization, immutability, and full traceability, which can significantly enhance the transparency and credibility of financial audits [3–7]. Particularly in the context of the widespread adoption of mobile platforms, the integration of blockchain technology into financial audit tracking has become one of the most prominent research directions in both academia and industry.

The significance of this study lies in the exploration of a blockchain-based mobile platform financial audit tracking system, aimed at filling several gaps in current audit technologies and methods. Existing financial audit systems predominantly rely on traditional centralized databases, making it difficult to ensure the integrity and reliability of data throughout the audit process. The introduction of blockchain technology not only offers a decentralized ledger system, ensuring the security of financial data, but also enables the automation of the audit process through smart contracts, thus improving audit efficiency. Therefore, the development of a blockchain-based mobile platform financial audit tracking system can enhance the transparency and accuracy of the audit process while driving technological innovation in the global financial audit industry.

Although some studies have attempted to apply blockchain technology in the field of financial auditing, several limitations remain in existing research methodologies [8–12]. Firstly, many studies focus solely on the fundamental architecture design of blockchain technology, neglecting how it can be integrated with the user requirements of mobile platforms, particularly in terms of how financial audit tracking can be efficiently and conveniently performed on mobile devices [13–17]. Secondly, current study is often concentrated on the singular application of blockchain functions, lacking in-depth integration and optimization between blockchain and the financial audit information tracking mechanism [18–22]. Finally, the existing methodologies frequently face challenges in practical implementation, particularly with regard to performance and security, which still require improvement.

This study emphasizes two key points: the development of an efficient and secure blockchain system for mobile platforms and the implementation of a traceability mechanism for financial audit tracking using blockchain technology. This study not only offers new perspectives on blockchain applications in financial auditing but also provides theoretical groundwork and practical direction for financial audit tracking systems on mobile platforms, showcasing both academic significance and practical potential.

2 LAYERED STRUCTURE OF THE BLOCKCHAIN SYSTEM ON MOBILE PLATFORMS

The blockchain system structure for financial audit tracking on mobile platforms is primarily composed of six distinct components, as illustrated in Figure 1.

In the context of financial audit tracking applications, the primary task of the data layer is to ensure the integrity, transparency, and immutability of financial data. Each block in the blockchain contains the hash value of the previous block, as well as the audit data for the current block. This data structure guarantees both the chronological order of audit records and their immutability. Financial audit data on mobile platforms is stored using encryption techniques, with only authorized users being able to view or manipulate the data. Let the random numbers be denoted by v and e, and the generator of the cyclic group be represented by g^l. The corresponding encryption formula is as follows:

$$Z = g^l e^v MODv^2 \tag{1}$$

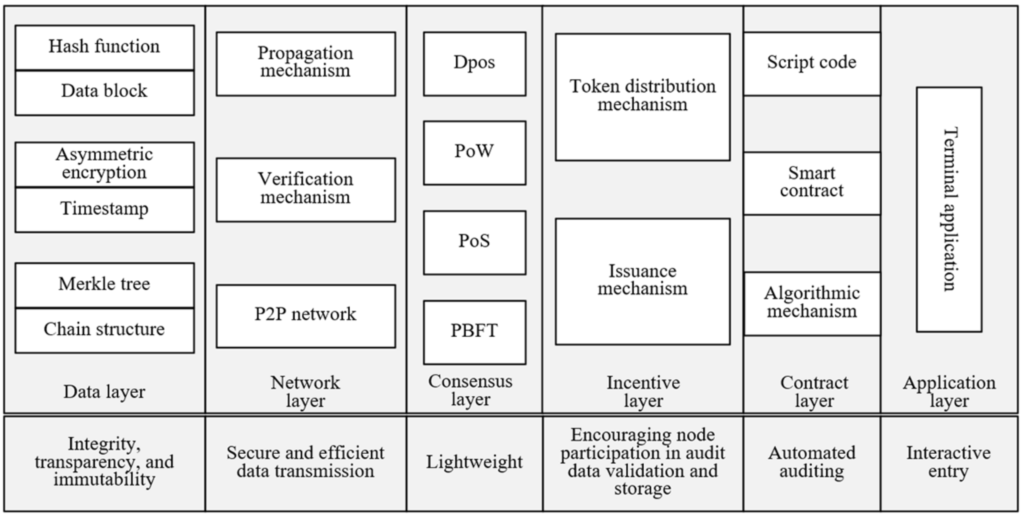


Fig. 1. Composition of the blockchain system for financial audit tracking on mobile platforms

The network layer must handle efficient connections between user devices and ensure the secure and efficient transmission of data. Particularly in the context of financial audit tracking, the network layer also needs to ensure the rapid synchronization of audit data across multiple nodes and provide robust resistance to interference. Given that mobile devices often face issues such as unstable networks and limited bandwidth, the network layer must optimize data transmission protocols to reduce latency while ensuring the integrity and confidentiality of audit data during its transmission. The design of the consensus mechanism must ensure that the system can quickly and reliably verify and record audit data, preventing malicious tampering and data forgery. To accommodate the resource constraints of mobile platforms, a lightweight consensus algorithm must be employed in the blockchain-based financial audit tracking system. These consensus algorithms can enhance transaction processing efficiency while maintaining security and reducing the computational burden on devices. Additionally, considering the high sensitivity of financial audits, stringent identity verification and audit permission controls should be incorporated into the consensus mechanism to ensure that only legitimate users are allowed to participate in the consensus process.

The incentive layer can be used to motivate nodes to participate in the validation and storage of audit data. For instance, auditors, system administrators, and other participants can be rewarded by engaging in data verification, maintenance, and audit processes within the blockchain network, thereby ensuring the continuous operation of the blockchain system and encouraging participant engagement. The incentive mechanism can be realized through token rewards, resource sharing, or point-based systems to motivate various roles. For mobile platforms, the incentive layer must consider the resource limitations of devices, designing low-consumption, high-benefit incentive schemes to ensure that the system's economic model promotes active participation while maintaining the independence and objectivity of the audit process. Smart contracts can automate the execution and verification of audit tasks. For example, after the completion of an audit task, a smart contract can automatically generate an audit report or trigger relevant notification mechanisms. By using smart contracts, the system can realize efficient automated auditing processes, reducing human intervention and improving audit efficiency and transparency. For mobile platform applications, smart contracts must possess high execution efficiency and low latency to accommodate the computational and network environments of mobile devices. The smart contract layer is not limited to the automatic execution of audit tasks; it can also be designed to automatically handle the validation and compliance checks of audit data, ensuring that financial data complies with relevant regulations and standards. The application layer is primarily used to provide the entry point for users to interact with the blockchain, including functions such as viewing audit data, tracking the audit process, and generating audit reports. Given that the system is intended for use on mobile platforms, particular attention must be paid to user experience design to ensure that operations on mobile devices are intuitive and seamless. The application layer must also efficiently interface with the underlying blockchain technology, supporting cross-platform data synchronization and operational verification. Additionally, the application layer should incorporate functions such as real-time notifications, data backup, and audit task management, ensuring the efficiency and timeliness of the financial audit process.

In the blockchain system for financial audit tracking on mobile platforms, the design of the consensus algorithm must take into account the high reliability, transparency, and immutability of audit data while also accommodating the resource constraints of mobile devices and the unstable network environment. Traditional blockchain consensus algorithms typically focus on handling large-scale transactions and enhancing system security, but these algorithms may encounter issues such as high energy consumption, inefficiency, and excessive latency when applied on mobile platforms. Additionally, the financial audit process generally requires a high degree of transparency and immutability of data, which imposes stricter demands on the blockchain consensus algorithm. In response to these issues, improvements to the consensus algorithm of the blockchain system for financial audit tracking on mobile platforms may be necessary to enhance system efficiency and adaptability.

The following outlines the detailed steps for improving the consensus algorithm of the blockchain system in the context of financial audit tracking:

Step 1: Client data upload to the blockchain: The first step involves uploading all relevant financial data to the blockchain through the client. Given the limited storage and computational capabilities of mobile devices, data preprocessing and compression must be performed on the client side to ensure that the size of the uploaded data meets the blockchain's storage requirements. Additionally, the client must support encryption technologies to ensure the privacy and security of the data during transmission. Particular attention must be paid to the data format and the accurate recording of timestamps in this step to ensure that the source and changes of each data entry can be precisely traced during subsequent audits.

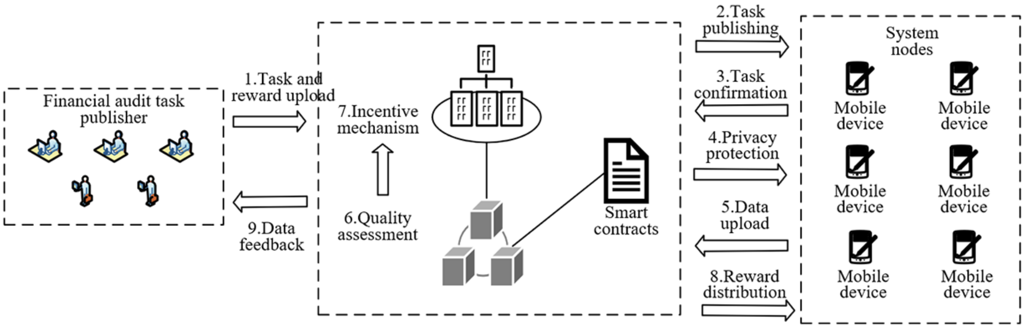


Fig. 2. Blockchain-based financial audit mobile platform architecture

Step 2: Validation and processing by the main node: Once the data is uploaded to the blockchain network, validation and processing can be performed by the main node. Figure 2 illustrates the architecture of the blockchain-based financial audit mobile platform. For financial audit data, the main node must not only check the correctness of the data format but also conduct compliance checks in accordance with predefined audit rules to ensure that the transaction data meets financial audit standards. Given the stringent requirements of financial audits, the validation process at the main node must guarantee both the accuracy and consistency of the data, allowing the true nature of each financial operation to be clearly reflected during audits. If any anomalies or non-compliant data are detected by the main node, they are promptly flagged, and the system administrator or auditor is notified for manual review.

Step 3: Selection of consensus nodes and optimization of network efficiency: To accommodate the resource limitations of the mobile platform and the instability of the network environment, the system prioritizes nodes with favorable network conditions and credit status when selecting consensus nodes. Specifically, each node is evaluated based on factors such as network latency, bandwidth, and historical performance, with preference given to nodes that exhibit low latency, high stability, and strong processing capabilities. To counteract the volatility of the mobile platform's network environment, the system can also configure multiple fault-tolerant nodes to prevent consensus failures during network instability.

Step 4: Determination of consensus node acquisition: In the context of financial audit tracking, ensuring the participation of a sufficient number of consensus nodes is critical, as these nodes collectively verify and store the financial audit data, ensuring its transparency and immutability. To maintain the accuracy and security of audit data, the system must ensure a balanced and decentralized distribution of nodes during the selection process, thereby preventing single points of failure and security risks associated with centralized nodes.

Step 5: Initial node credit and latency index evaluation: In financial audit applications, the credit status of nodes directly affects the speed and accuracy of audit data verification. For the network's initial nodes, as no consensus-related information has yet been gathered, it is not possible to directly access node credit through consensus behavior. In such cases, the system allocates an initial credit value to each node by measuring its network latency, represented by the z-value. The latency index, ID, serves as a critical factor in credit evaluation, helping the system identify nodes with rapid responses and good network quality. Assuming the minimum network latency is represented by z_{MIN}, the expression for the initial credit value $T_{(IN)}$ is given by:

$$T_{(IN)} = \begin{cases} \dfrac{100 - z}{100 - z_{MIN}}, z < 100lt \\ -1, z \geq 100lt \end{cases} \tag{2}$$

The consensus credit value, $T_{(ON)}$, is determined by the current state of the blockchain network and the node's performance during the consensus process. The consensus result is represented by $H_{(RE)}$, and the confirmation messages sent by different nodes during the consensus process are denoted as $H_{(CO)}$. The comparison results are represented by CP, with the weight being denoted as i. The credit assignment and network status during the consensus process were quantified by $T_{(ON)}$. After multiple rounds of consensus processing, the global node credit, $T_{(LA)}$, was obtained. To determine whether a node is trustworthy, the system compares $H_{(RE)}$ and $H_{(CO)}$ after completing a consensus process. The corresponding formulas are as follows:

$$CP = \begin{cases} 0, T_{(IN)} H_{(RE)} \neq H_{(CO)} \\ 1, T_{(IN)} H_{(RE)} = H_{(CO)} \end{cases} \tag{3}$$

$$T_{(ON)} = Z + i(CP - ID) \tag{4}$$

Furthermore, the value of $T_{(LA)}$ was used to classify all nodes based on their creditworthiness. The classification result, $T_{(CA)}$, is expressed as:

$$T_{(CA)} = \begin{cases} 1, T_{(LA)} > \sum_{u=0}^{v-1} T_{(ON)}^{u} \\ 2, \sum_{u=0}^{v-1} T_{(ON)}^{u} > T_{(LA)} > \sum_{u=0}^{v-1} T_{(ON)} - T_{(IN)} \\ 3, = \sum_{u=0}^{v-1} T_{(ON)}^{u} > T_{(LA)} \end{cases} \tag{5}$$

Nodes exhibiting Byzantine faults under any network condition were replaced by alternative nodes, and they were removed from the pool of critical nodes.

3 IMPLEMENTATION OF FINANCIAL AUDIT INFORMATION TRACKING

The mobile platform blockchain-based financial audit tracking solution aims to enhance data transparency, immutability, and efficiency within the financial audit process while addressing the challenges posed by limited resources on mobile devices and unstable network environments. To achieve this, the system first encrypted all financial transaction data on the client side before uploading it to the blockchain. Smart contracts were then used to automatically execute audit rules, ensuring that the data complies with financial standards. When uploading data, lightweight encryption techniques were employed to conserve computational resources, and preprocessing and compression were applied to reduce the bandwidth requirements for data transmission. After data was uploaded, the primary node was responsible for the initial validation of the data, confirming its legality and consistency, while consensus nodes further verified the data using the optimized consensus algorithm. A mechanism was specifically designed to select consensus nodes based on node credit values and network latency indices, ensuring that the system can efficiently validate and record data in unstable network environments while minimizing bandwidth and computational resource wastage. Figure 3 illustrates the blockchain-based financial audit information tracking architecture on the mobile platform. The following are the detailed steps for implementing blockchain-based financial audit tracking on the mobile platform:

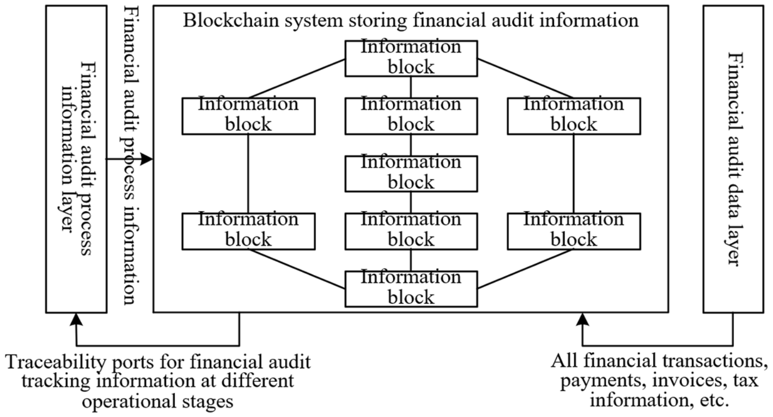

Financial audit process information layer
Financial audit process information
Blockchain system storing financial audit information
Information block
Information block
Information block
Information block
Information block
Information block
Information block
Information block
Financial audit data layer
Traceability ports for financial audit tracking information at different operational stages
All financial transactions, payments, invoices, tax information, etc.

Fig. 3. Blockchain-based financial audit information tracking architecture on the mobile platform

Step 1: Data collection and recording: All financial data must be meticulously recorded, ensuring that it is promptly uploaded to the blockchain. Initially, the existing financial management system needs to be integrated with the blockchain platform. This includes interfacing with accounting software, payment systems, and bank APIs, ensuring that all financial transactions, payments, invoices, taxes, and other information can be automatically retrieved and recorded within the system. To ensure the timeliness of the audit, financial data must be collected in real time. This may require the addition of a data collection module within the existing financial system to immediately transmit the details of each transaction to the blockchain. During the data collection process, to guarantee the security and immutability of the data, each financial transaction must undergo digital signing and encryption. The signature ensures the authenticity and source of the data, while encryption ensures the security of the data during transmission and storage.

The established financial audit information set F is defined as:

$$F = \begin{bmatrix} f_{11}, f_{12}, f_{13}, \ldots, f_{1v} \\ f_{21}, f_{22}, f_{23}, \ldots, f_{2v} \\ \vdots \quad \vdots \quad\quad \vdots \\ f_{l1}, f_{l2}, f_{l3}, \ldots, f_{lv} \end{bmatrix} \tag{6}$$

Step 2: Information upload to blockchain: Once the financial data collection is complete, the next step is to upload the data to the blockchain system. Considering the storage limitations of blockchain, the financial data must be appropriately packetized and compressed. Prior to uploading, the system can design a reasonable data packetization mechanism based on the transaction size, complexity, and upload frequency to reduce the pressure on network bandwidth. Before each financial transaction is uploaded, the system automatically validates it through a smart contract. This validation includes verifying the legitimacy of the transaction, the consistency of the data, and whether the audit rules are triggered. Once the data is recorded on the blockchain, it cannot be altered or deleted.

Step 3: Execution of smart contracts: The enterprise must design and write the rules for the smart contracts based on the financial audit requirements and industry standards. These rules may include automatically auditing the compliance of transactions, detecting unreasonable expenditures or income, and automatically generating audit reports. Smart contracts are capable of executing automatically based on predefined rules and conditions. Each step in the execution of the smart contract is recorded on the blockchain, ensuring that every audit decision can be tracked. Any individual can query the system to access the audit process and results, thereby ensuring the fairness and transparency of the audit.

Step 4: Audit information sharing: The decentralized nature of blockchain ensures that each financial record is synchronously stored across multiple nodes, guaranteeing that all auditors and management, regardless of their location, can access the latest audit data in real time. Once all financial transactions and audit data are recorded on the blockchain, they can be queried and viewed by all authorized users. Due to the chain structure of the blockchain, any changes to the data can leave a permanent record, ensuring the traceability of historical data. Auditors can query the detailed information of any transaction at any time, even tracing it back to the original data source.

Step 5: Anomaly monitoring and early warning: The system must implement real-time monitoring of financial data, using an automated rule engine to analyze and detect potential anomalies. Monitoring rules may include whether the transaction amount exceeds the budget, whether both parties in the transaction comply with the contract terms, whether duplicate payments exist, and whether abnormal large financial flows occur. These rules can be customized to meet the specific needs of the enterprise. Once the system identifies an anomalous transaction or potential risk behavior, the early warning mechanism should be immediately triggered. Various methods can be used for the warning, such as emails, text messages, or app notifications, to promptly alert the relevant parties. Furthermore, the system can automatically initiate subsequent investigation or response processes based on the anomaly type, such as triggering an automated audit report, temporarily freezing the data, or restricting access.

4 EXPERIMENTAL RESULTS AND ANALYSIS

Table 1. Fault tolerance performance results of the consensus algorithm

Downtime Occurrences	Node Id	Data Received	Final Data
0	01	1011	1
	02	1111	1
	03	1011	1
1	01	1001	1
	02	0100	1
	03	1010	1
2	01	1001	*null*
	02	1010	*null*
	03	0110	*null*
3	01	0010	*null*
	02	110	*null*
	03	0110	*null*

Based on the experimental data presented in Table 1, it can be observed that as the number of downtimes increases, the stability and data consistency of the nodes gradually decline. In the initial stage (with zero downtimes), all three nodes (01, 02, 03) successfully retrieve and transmit correct audit data, with the final data being consistent and equal to 1. This indicates that, in the absence of downtime, the system can maintain good data consistency. However, as the number of downtimes increases (to 1, 2, and 3), significant issues arise regarding data consistency and integrity. For example, when the downtime count reaches 2, the final data for nodes 01, 02, and 03 are all marked as null, indicating that, under high downtime frequencies, certain nodes are unable to recover or transmit valid data. When the downtime count reaches 3, the final data for all nodes is null, further demonstrating that an increase in node downtimes directly leads to data unavailability, challenging the fault tolerance of the system. It can be concluded that the current consensus algorithm exhibits vulnerability when faced with multiple node downtimes, particularly when the downtime count reaches 2 or more, as some nodes are unable to successfully recover the data, thereby threatening the overall data consistency of the system. Therefore, by improving the consensus algorithm, the system's high availability and consistency can be ensured in the event of node failures. The advantage of Byzantine fault tolerance algorithms lies in their ability to tolerate up to 50% faulty nodes.

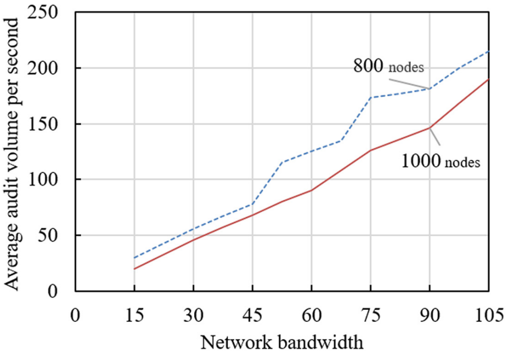
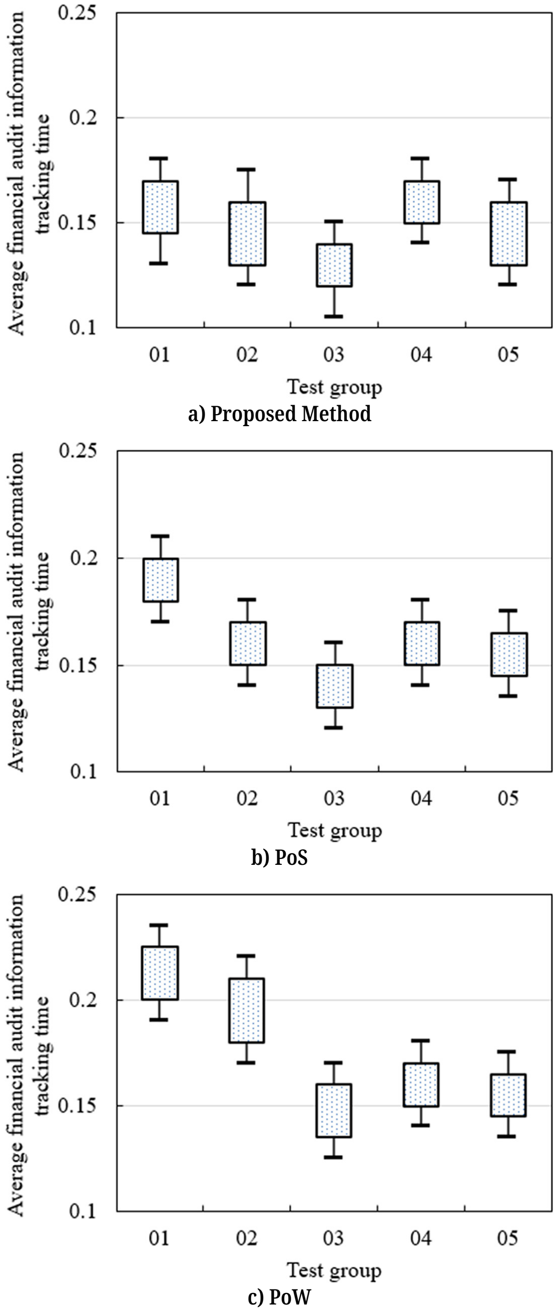


Fig. 4. Experimental results of the financial audit efficiency of the system

From Figure 4, it can be observed that the number of nodes (800 and 1000) has a significant impact on the financial audit efficiency under different mobile network bandwidth conditions (ranging from 0 to 105 Mbps). As the bandwidth increases, the tracking time of audit data decreases progressively. However, the effect of increasing the number of nodes on performance differs. In the case of 800 nodes, as the bandwidth increases from 0 Mbps to 105 Mbps, the tracking time decreases significantly from 200 ms to 43 ms, indicating that the expansion of bandwidth has a marked effect on improving system efficiency. However, when the number of nodes increases to 1000, the tracking time slightly increases under the same bandwidth conditions. For example, at a bandwidth of 60 Mbps, the tracking time for 800 nodes is 115 ms, while for 1000 nodes, the tracking time increases to 126 ms. This indicates that, with a higher number of nodes, although the system can still maintain relatively high efficiency, network bandwidth limitations may lead to increased latency. Overall, it can be concluded that the balance between network bandwidth and the number of nodes is crucial for system efficiency. In the blockchain-based financial audit tracking system on mobile platforms, network bandwidth is identified as a key factor influencing audit efficiency, while an increase in the number of nodes may result in a decrease in efficiency. However, optimized design can effectively mitigate this issue. The experiment demonstrates that the proposed method can maintain high performance under various network conditions, particularly when 800 nodes are used. With an increase in bandwidth, the system's tracking efficiency is significantly improved. This validates the efficiency and flexibility of the optimized blockchain group-layer structure in audit information tracking. Furthermore, although an increase in the number of nodes results in some delay, the overall performance of the system remains stable.



a) Proposed Method

b) PoS

c) PoW

Fig. 5. Experimental results of average financial audit information tracking time for different consensus methods

According to the test group data of different consensus algorithms shown in Figure 5, the performance of the three consensus algorithms in the financial audit information tracking process varies. In the test group using the proposed method, the maximum values, upper quartiles, and medians of all test groups exhibit relatively low time consumption. In particular, the maximum values and upper quartiles are generally below 0.18 seconds, indicating that the proposed method maintains good consistency and still achieves short response times under higher loads. In contrast, in the proof of stake (PoS) and proof of work (PoW) test groups, the time for the maximum values is slightly higher (the maximum value for PoS is 0.21 seconds, and for PoW, it is 0.235 seconds). Although the performance of these algorithms is similar in terms of upper quartiles and medians, the maximum and minimum values fluctuate significantly, demonstrating that under high-load conditions, time consumption increases. This indicates that the optimized design method offers a clear advantage in terms of time consumption, effectively handling financial audit data tracking tasks. It can be concluded that the optimized blockchain technology proposed in this study has undergone effective optimization for the information tracking scheme, resulting in significant improvements in overall performance. A comparison of the test group using the proposed method with the test results of the PoS and PoW algorithms shows that the optimized blockchain design significantly reduces the time consumption in the information tracking process, particularly maintaining stability under high loads.

Table 2. Performance comparison of different consensus methods in financial audit information tracking

Performance	Proposed Method	PoS	PoW
Regulatory capability	High	Moderate	Low
Information security	High	Low	Moderate
Information integrity	High	Low	Moderate
Traceability	High	Moderate	Moderate
Trustworthiness of information track results	High	Moderate	Low

The data presented in Table 2 illustrates significant performance differences between various consensus algorithms in the financial audit information tracking system. The optimized blockchain method proposed in this study demonstrates outstanding performance across all key performance indicators, particularly in regulatory capability, information security, information integrity, traceability, and the trustworthiness of the information tracking results. These findings indicate that the optimized consensus method can effectively ensure the security and integrity of data during the financial audit data tracking process while also maintaining efficiency and trustworthiness in the auditing procedure. In comparison, the performance of the PoS and PoW algorithms is generally moderate or lower, particularly in terms of information security, information integrity, and the trustworthiness of the information tracking results. The security of PoS is lower, while the trustworthiness of PoW does not reach a high level. This suggests that while PoS and PoW can achieve data tracking under certain conditions, they exhibit significant flaws in ensuring the security and trustworthiness of audit data, failing to meet the high standards required for financial auditing. It can be concluded that the optimized blockchain technology solution exhibits clear advantages in the financial audit information tracking process, particularly in terms of regulatory capability, information security, and trustworthiness, where it outperforms traditional PoS and PoW methods.

5 CONCLUSION

An optimized blockchain-layered structure and financial audit tracking mechanism were proposed and investigated in this study. The focus was on the efficiency, security, and traceability of financial audits on mobile platforms. Experimental results show that the proposed method outperforms traditional consensus algorithms, such as PoS and PoW, in terms of fault tolerance, audit efficiency, and information tracking performance. Notably, in terms of average data traceability time and trustworthiness, the optimized solution demonstrates significant advantages, better accommodating the high-frequency and high-load demands of financial audits. Through the application of blockchain technology, effective tracking and verification of the entire financial audit process were achieved, enhancing the transparency and traceability of information, thus improving the overall security and reliability of the system.

However, certain limitations exist in this study. Firstly, while the experimental results indicate the superiority of the proposed method across various performance indicators, further validation of the system's scalability and its capacity to handle extreme network conditions is required for real-world large-scale applications. Secondly, the optimized blockchain solution has higher requirements for hardware and network bandwidth, which could lead to performance bottlenecks in resource-limited environments. Future research could explore the following directions: a) further optimization of the consensus algorithm to improve efficiency and fault tolerance in low-resource environments; b) development of more flexible blockchain architectures tailored to diverse financial audit scenarios, capable of addressing various types of audit tasks; and c) exploration of integrating technologies such as artificial intelligence to enhance the system's capacity for large-scale data analysis and intelligent decision support.

6 REFERENCES

[1] Z. B. Lazarevska, T. Tocev, and I. Dionisijev, "How to improve performance in public sector auditing through the power of big data and data analytics? – The case of the Republic of North Macedonia," *Journal of Accounting, Finance and Auditing Studies*, vol. 8, no. 3, pp. 187–209, 2022. https://doi.org/10.32602/jafas.2022.023

[2] L. Sabauri, "Internal audit's role in supporting sustainability reporting," *International Journal of Sustainable Development and Planning*, vol. 19, no. 5, pp. 1981–1988, 2024. https://doi.org/10.18280/ijsdp.190537

[3] E. Pimentel, E. Boulianne, S. Eskandari, and J. Clark, "Systemizing the challenges of auditing blockchain-based assets," *Journal of Information Systems*, vol. 35, no. 2, pp. 61–75, 2021. https://doi.org/10.2308/ISYS-19-007

[4] A. Mwange and M. Chansa, "Emerging issues in accounting: A theoretical review," *Journal of Accounting, Finance and Auditing Studies*, vol. 8, no. 4, pp. 172–196, 2022. https://doi.org/10.32602/jafas.2022.032

[5] B. L. Handoko, D. S. Indrawati, and S. R. P. Zulkarnaen, "Embracing AI in auditing: An examination of auditor readiness through the tram framework," *International Journal of Computational Methods and Experimental Measurements*, vol. 12, no. 1, pp. 53–60, 2024. https://doi.org/10.18280/ijcmem.120106

[6] O. Senturk and A. Baghırov, "Enhancing sustainable development through blockchain: A study on risk management and data integrity," *Journal of Organizations, Technology and Entrepreneurship*, vol. 1, no. 2, pp. 110–126, 2023. https://doi.org/10.56578/jote010204

[7] U. Nikonenko, D. Maksymenko, V. Holovachko, Y. Golubka, and O. Guk, "Accounting and auditing time management: A model for enterprise sustainable development planning," *International Journal of Sustainable Development and Planning*, vol. 18, no. 9, pp. 2883–2889, 2023. https://doi.org/10.18280/ijsdp.180926

[8] M. El Ghazouani, A. Ikidid, C. Ait Zaouiat, L. Aziz, M. Y. Ichahane, and L. Er-Rajy, "Optimal method combining blockchain and multi-agent system to ensure data integrity and deduplication in the cloud environment," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 10, pp. 90–105, 2024. https://doi.org/10.3991/ijim.v18i10.43305

[9] S. Galanti and Ç. Y. Özsoy, "Can blockchain help improve financial inclusion? A comparative study," *Journal of Economic Issues*, vol. 57, no. 2, pp. 438–449, 2023. https://doi.org/10.1080/00213624.2023.2200650

[10] S. Schuetz and V. Venkatesh, "Blockchain, adoption, and financial inclusion in India: Research opportunities," *International Journal of Information Management*, vol. 52, p. 101936, 2020. https://doi.org/10.1016/j.ijinfomgt.2019.04.009

[11] A. Miah, M. Rahouti, S. K. Jagatheesaperumal, M. Ayyash, K. Xiong, F. Fernandez, and M. Lekena, "Blockchain in financial services: Current status, adoption challenges, and future vision," *International Journal of Innovation and Technology Management*, vol. 20, no. 8, p. 2330004, 2023. https://doi.org/10.1142/S0219877023300045

[12] Y. Souissi, F. Ezzi, and A. Jarboui, "Blockchain adoption and financial distress: Mediating role of information asymmetry," *Journal of the Knowledge Economy*, vol. 15, pp. 3903–3926, 2024. https://doi.org/10.1007/s13132-023-01263-3

[13] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, vol. 158, p. 120166, 2020. https://doi.org/10.1016/j.techfore.2020.120166

[14] Y. Wang, D. K. Kim, and D. Jeong, "A survey of the application of blockchain in multiple fields of financial services," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 935–958, 2020. https://doi.org/10.3745/JIPS.04.0185

[15] W. Gao and C. Su, "Analysis of earnings forecast of blockchain financial products based on particle swarm optimization," *Journal of Computational and Applied Mathematics*, vol. 372, p. 112724, 2020. https://doi.org/10.1016/j.cam.2020.112724

[16] V. Blikhar, H. Lukianova, I. Komarnytska, M. Vinichuk, and V. Gapchich, "Problems of normative and legal regulation of the process of applying blockchain technology in the financial system of Ukraine," *Financial and Credit Activity Problems of Theory and Practice*, vol. 3, no. 50, pp. 410–418, 2023. https://doi.org/10.55643/fcaptp.3.50.2023.4088

[17] L. Mishra and V. Kaushik, "Application of blockchain in dealing with sustainability issues and challenges of financial sector," *Journal of Sustainable Finance & Investment*, vol. 13, no. 3, pp. 1318–1333, 2023. https://doi.org/10.1080/20430795.2021.1940805

[18] J. Su, L. He, R. Ren, and Q. Liu, "Reliable blockchain-based ring signature protocol for online financial transactions," *KSII Transactions on Internet & Information Systems*, vol. 17, no. 8, pp. 2083–2100, 2023. https://doi.org/10.3837/tiis.2023.08.007

[19] A. Alenizi, S. Mishra, and A. Baihan, "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Engineering Journal*, vol. 15, no. 6, p. 102733, 2024. https://doi.org/10.1016/j.asej.2024.102733

[20] R. Mavilia and R. Pisani, "Blockchain and catching-up in developing countries: The case of financial inclusion in Africa," *African Journal of Science, Technology, Innovation and Development*, vol. 12, no. 2, pp. 151–163, 2020. https://doi.org/10.1080/20421338.2019.1624009

[21] S. Gupta, S. Modgil, T. M. Choi, A. Kumar, and J. Antony, "Influences of artificial intelligence and blockchain technology on financial resilience of supply chains," *International Journal of Production Economics*, vol. 261, p. 108868, 2023. https://doi.org/10.1016/j.ijpe.2023.108868

[22] E. Ducas and A. Wilner, "The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada," *International Journal: Canada's Journal of Global Policy Analysis*, vol. 72, no. 4, pp. 538–562, 2017. https://doi.org/10.1177/0020702017741909

7 AUTHOR

Eying Liu, a graduate of Hunan University with a Master's degree in management, is currently working at Hunan International Economics University. Her primary area of study focuses on accounting information technology and financial management (E-mail: wuyueyuhan@163.com; ORCID: https://orcid.org/0009-0009-3695-1477).