Eng Int Syst (2025) 4: 457–467


**Engineering**
***Intelligent Systems***

# Key Technologies for Financial Data Security Protection Based on Blockchain

**Su Meng**[1]*

[1] *Shenyang Institute of Engineering, Shenyang 110000, Liaoning, China*

The centralized database structure of the traditional financial system has significant risks in terms of audit and internal control, increasing its vulnerability to hacker attacks and making it difficult to trace and audit data. In addition, data privacy protection is inadequate and there is a high risk of information leakage. This study used the decentralized and tamper-proof characteristics of blockchain technology (BT) to improve the security and credibility of financial data in audit and internal control. The research used distributed storage to ensure data anti-attack capabilities, and smart contracts automatically perform data verification and management operations to reduce the impact of human intervention on the internal control process. Data encryption is combined with zero-knowledge proof methods to achieve privacy protection. Timestamp-based traceability and audit mechanisms are designed to ensure financial data compliance and verifiability. In terms of data consistency between nodes, the PBFT (practical Byzantian Fault Tolerance) consensus algorithm is used to optimize the efficiency of financial information synchronization, and the accurate access of authorized users in financial and audit activities is guaranteed through the role-based authority control system. Experimental results show that the blockchain-based solution has a successful interception rate of more than 90%, and a data integrity verification pass rate of 100%, while the interception rate of the traditional DES (Data Encryption Standard) encryption solution does not exceed 70%. In regard to data privacy protection, the leakage rate of the zero-knowledge proof mechanism is only 0.35%, which is better than the 3% of RSA (Rivest-Shamir-Adleman) encryption. For financial data tracing and auditing, the average tracing time of BT is 0.46 seconds, which is significantly better than the 2.22 seconds of traditional databases. The comprehensive evaluation results show that BT has excellent anti-attack ability, data privacy protection performance and financial data management efficiency in audit and internal control, and is expected to play an important role in a wider range of financial management applications.

Keywords: Financial Data Security Protection, Blockchain Technology, Data Privacy Protection, Smart Contracts, Attack Resistance Capability

## 1. INTRODUCTION

The rapid development of blockchain technology has brought unprecedented technological changes to data security, privacy protection, and decentralization. Its distributed storage and tamper-proof features have been widely used in many fields [1–2]. Traditional financial information systems rely on centralized database structures to handle data storage and management, which are vulnerable to external malicious attacks and have high data security risks [3–4]. With the frequent occurrence of data leakage incidents [5], the issue of financial data security has gradually received attention. Traditional financial systems have shortcomings in terms of data tamper-proofing and traceability, making it difficult to ensure the authenticity and reliability of data and meet high privacy protection requirements. Existing systems cannot provide effective encryption and access control methods for privacy protection, and data privacy protection is inadequate [6]. Traditional financial systems face audit difficulties because the audit process relies on manual records and complex data analysis operations, resulting in poor audit efficiency and insufficient credibility [7]. The demand for decentralized security, privacy protection, and traceability is increasing, and blockchain technology offers breakthrough improvement potential to the management of financial data [8]. The application of blockchain technology in the field of financial data management and the adoption of key technical

*Corresponding Author. Email: mlms990@126.com

means such as distributed storage, smart contracts, encryption technology, consensus algorithms, etc., to achieve secure management of financial data, is an important means of solving the problems inherent in traditional financial systems.

In this study, innovative solutions for key technologies of financial data security protection based on blockchain are designed to address challenges such as data storage, privacy protection, traceability, and auditing in traditional financial systems. The study adopted distributed storage architecture to store financial data in multiple nodes, improve anti-attack capabilities, and reduce the risk of data leakage. Based on the automated execution mechanism of smart contracts, the study designed a data verification and management process without human intervention to ensure the integrity and security of financial data. For privacy protection, the study introduces zero-knowledge proof methods to achieve transaction privacy protection, combining efficient encryption algorithms to ensure the confidentiality of data during transmission and storage. The study also enhances data transparency and traceability through a timestamp-based traceability and audit mechanism to meet regulatory compliance requirements. This study used the PBFT consensus algorithm to ensure data consistency between nodes in the blockchain network and ensure data accuracy and reliability. The precise access mechanism based on the role-based permission control model ensures the refined data access rights of authorized users and effectively reduces the risk of information leakage.

## 2. RELATED WORK

In recent years, the application of BT capabilities to data security, privacy protection and system anti-attack has received widespread attention. Liu et al. adopted a distributed access control system based on BT, combined with fog computing and consortium chain concepts, as well as MLNCML (mixed linear and nonlinear spatiotemporal chaotic systems) and LSB (least significant bit) encryption methods to solve the problem of IoT (Internet of Things) data security transmission [9]. Da Xu et al. used a system analysis method to explore the current application status of BT in IoT security. The study pointed out that BT can improve the security performance of IoT [10]. Liu et al. designed a survey verification form for blockchain and mobile terminal privacy protection, which made up for the lack of empirical research on e-commerce trust behavior [11]. Lohith et al. studied the prospect of combining blockchain with big data to overcome the data reliability problem of artificial intelligence systems, and concluded that this combination can ensure data integrity, improve record efficiency, and ensure secure data sharing among multiple parties [12]. Maariz et al. comprehensively evaluated the data integrity indicators of mainstream blockchain networks such as Bitcoin, Ethereum, and Hyperledger Fabric, analyzed the impact of BT on the data integrity and security of digital environments, and found the differences in immutability and reliability of each platform, as well as their respective security characteristics, providing guidance for the selection of blockchain platforms [13]. Namperumal et al. explored the role of blockchain technology in enhancing data integrity and transparency in cloud-based human capital management (HCM) solutions through research and analysis methods and found that blockchain technology can significantly improve data security, integrity, and transparency [14]. Tatineni explored the way that the integration of blockchain technology and data science can address the challenges of data security and transparency, and found that this integration can strengthen data security, ensure data integrity, and improve data-sharing transparency [15]. These studies have made significant progress in their respective fields, but in the context of financial data management, most studies still have problems with insufficient integration and unstable performance in terms of data storage, privacy protection, and traceability auditing.

Existing research has used a variety of methods to improve the security protection of financial data [16]. By integrating artificial intelligence and BT, Olubusola et al. explored how the two can work together to improve the security of financial services and found that this integration can enhance transaction trust, effectively detect and prevent fraudulent activities, optimize identity authentication, and ensure compliance [17]. Jimmy used a research and analysis method to determine whether BT can solve the data security challenges faced by financial institutions. The study found that BT plays a significant role in ensuring the security of financial data[18]. Li et al. used a system analysis method to study the application status and challenges of BT in the financial and economic fields, and proposed constructive suggestions to promote the development of BT in these fields [19]. Rijanto investigated the way that BT can solve automation problems in supply chain finance (SCF) based on the Technological Acceptance Model (TAM). The results showed that the advantages of BT such as trust, effectiveness and distributed ledger transaction data are the main factors driving its adoption [20]. Lingling proposed an information management framework based on blockchain and the Internet of Things using theoretical framework construction and technical design methods to solve the problem of information asymmetry in supply chain finance, and verified its effectiveness through theoretical analysis [21]. Mustyala used a combination of theoretical analysis and practical cases to investigate whether BT can be integrated into financial technology infrastructure to strengthen security and trust, and concluded that blockchain can effectively reduce fraud risks and improve the operational security and efficiency of financial technology companies [22]. George used industry report analysis and technology integration research to determine how AI (Artificial Intelligence), blockchain and machine learning technologies can work together to improve the cybersecurity defense of new banks, and concluded that the combination of these technologies can effectively respond to current and future threats and ensure the safety of banks and consumers [23]. Becherer M proposed a trusted collaboration framework that achieves verifiability and security of multi-party collaboration through blockchain smart contracts, which echoes research in the field of financial data security protection[24]. These methods have achieved some results in financial data protection, but there is still room for improvement in terms of privacy, data-sharing and consistency.

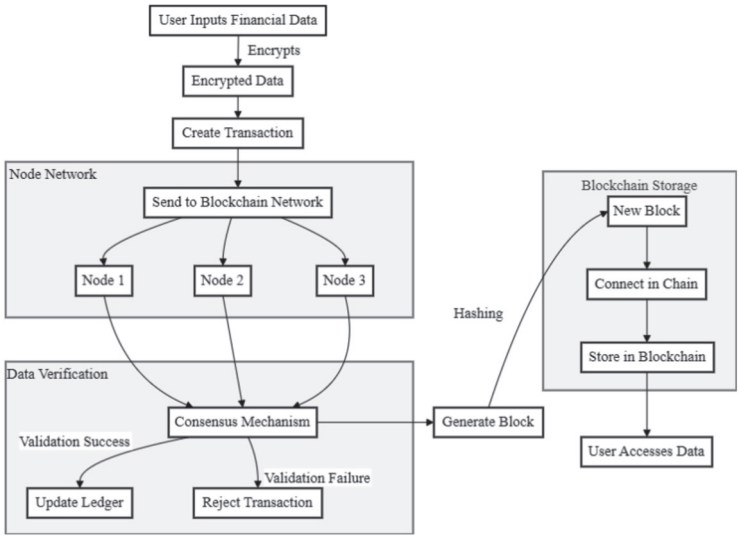


**Figure 1** Depiction of blockchain financial data storage structure.

# 3. BLOCKCHAIN-BASED DATA SECURITY PROTECTION SCHEME

## 3.1 Application of BT in Financial Data Storage

In the field of financial data storage, the traditional centralized database structure has significant security risks. Centralized storage makes data vulnerable to hacker attacks, and data recovery is cumbersome when lost or damaged. Using BT to build a distributed storage system is an effective way to solve this problem. The distribution and storage of financial data in multiple blockchain nodes can significantly reduce the risks associated with centralization, and can improve the data's ability to resist attacks. The blockchain network structure and data storage process are shown in Figure 1:

In the specific implementation, Hyperledger Fabric is selected as the blockchain platform [25]. The platform allows the construction of multi-node distributed ledgers, forming a decentralized network environment by distributing data to different nodes. Each node has a complete copy of the ledger, ensuring that when some nodes are attacked, the overall data remains safe and available. Hyperledger Fabric provides a modular architecture design that allows the network to flexibly expand and adapt to the storage needs of financial data of different scales.

In the data storage operation, the transaction data is recorded in blocks in chronological order using a chain structure. Each block is connected to the previous block through an encryption algorithm to form an unalterable chain. The SHA-256 hash algorithm is used for data encryption to ensure the security of data during transmission and storage. The formula is used to represent the hash relationship of blocks in the chain:

$$H(B_n) = H(H(B_{n-1})||T_n||D_n) \tag{1}$$

where $H$ represents the hash function, $B_n$ is the current block, $T_n$ is the timestamp of the current block, and $D_n$ is the transaction data of the current block. This ensures that each block not only depends on the hash value of the previous block, but also contains its own timestamp and transaction information, enhancing data integrity and consistency.

To improve the security of decentralized storage, financial data is encrypted before entry. The symmetric encryption algorithm AES (Advanced Encryption Standard) is used to encrypt sensitive data to ensure that only authorized users can access the original data [26–27].

In the blockchain network, the communication between nodes is encrypted using the TLS (Transport Layer Security) protocol to ensure the security of data transmission [28]. The Merkle tree structure is used to enhance data verifiability. Before financial data is uploaded to the blockchain, a hash operation is performed first, and a root hash is generated through the Merkle tree. The root hash is then stored in the blockchain so that any node can verify the data integrity through the root hash. The Merkle tree construction formula is as follows:

$$H = H(H_1||H_2) \tag{2}$$

where $H_1$ and $H_2$ are the data hash values of the leaf nodes. By means of this structure, the system can quickly verify the consistency and integrity of the data.

## 3.2 Application of Smart Contracts in Data Automation Control

During implementation, smart contracts trigger corresponding operations through predefined conditions. When a financial transaction record is completed, the smart contract automatically generates an audit report and performs data verification. Figure 2 shows the workflow of smart contracts in financial data processing. After the user submits a transaction request, the system automatically controls the steps of input verification, executes a smart contract, updates financial data, and generates an audit report. In order to ensure the accuracy and consistency of data during contract execution, a strict input verification mechanism is implemented. When a user submits a transaction request, the smart contract checks the legitimacy of the input data

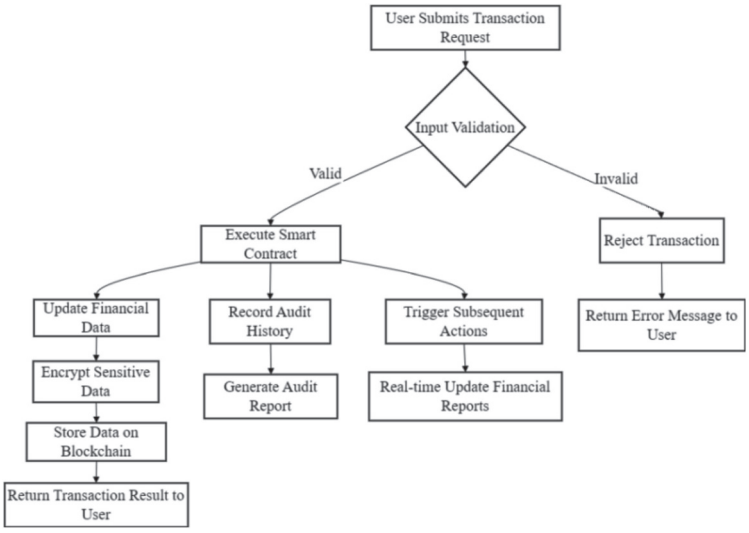


**Figure 2** Flowchart of the application of smart contracts in automated control of financial data.

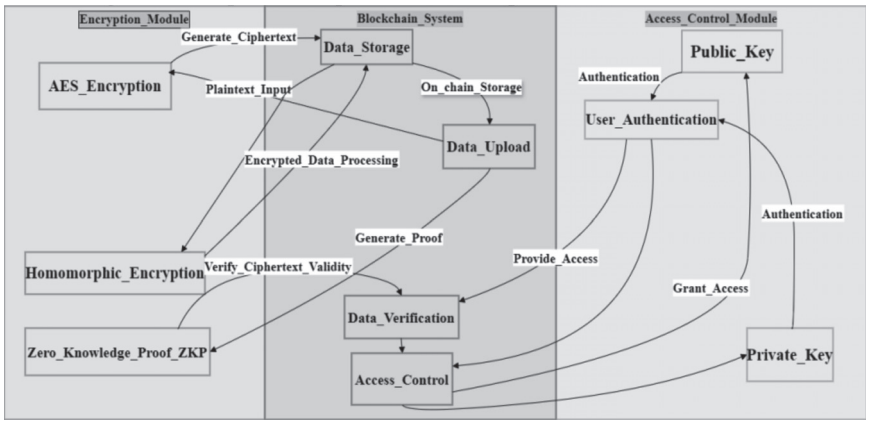


**Figure 3** Diagram of encryption and privacy protection architecture.

according to the set conditions, and any data that does not meet the conditions can be rejected. Logical judgment is exercised to ensure the quality of data entry. When recording financial data, if the input amount exceeds the set range, the smart contract can automatically reject the transaction.

Smart contracts can shorten the data update cycle and improve overall efficiency by processing multiple transactions in parallel [29]. The contract-triggering mechanism is designed so that when a transaction is successful, the system automatically performs subsequent operations. The mechanism enables the finance department to grasp the data dynamics in real time and ensure the timeliness and accuracy of information. The contract integrates audit tracking function so that each transaction has a complete audit record. Timestamps and transaction numbers are embedded in smart contracts to ensure that each transaction is traceable, and provide a detailed operation history. To ensure data privacy during the execution of smart contracts, symmetric encryption algorithms are used to safeguard sensitive data. Data encryption logic is included in the contract to ensure that only authorized users can decrypt and access sensitive information.

The application of smart contract technology improves the processing efficiency of automated control of financial data and enhances the security and transparency of data management. The system eliminates the risks of traditional centralized databases through the decentralized nature of blockchain. The immutability of the contract code ensures the safe execution of business logic. Any changes to contract terms must be verified and agreed to by network nodes to ensure the credibility of the data processing process.

## 3.3 Encryption Algorithm and Privacy Protection

Financial data is encrypted using the Advanced Encryption Standard (AES) to convert plaintext data into ciphertext, making it impossible for unauthorized access to decrypt the data [30]. The AES algorithm uses a symmetric key to encrypt and decrypt. Its encryption process is efficient and the data remains encrypted during both transmission and storage, making it difficult to decrypt sensitive data even if it is intercepted. The AES encryption process involves key expansion, byte replacement, row shift, column mixing, round key addition, etc. It uses a 128-bit or 256-bit key length to enhance the ability to resist brute force cracking.

Figure 3 depicts the encryption and privacy protection architecture. The financial system uses a homomorphic encryption scheme to perform partial data calculation and processing. The scheme allows operations such as addition

or multiplication to be performed on data in the ciphertext state, ensuring the convenience of operation in the encrypted state of the data and reducing the impact of the number of decryption times on performance. In the application scenario of homomorphic encryption, financial data is statistically analyzed in an encrypted state to avoid exposing decrypted data to the outside. The ciphertext can be $E(m)$, and encrypted homomorphic encryption still maintains the ciphertext state $E(m_1+m_2) = E(m_1)+E(m_2)$ after ciphertext addition, ensuring the invisibility of the original data. Multiplication homomorphism achieves the product operation on the chain without decryption through the multiplication operation of the ciphertext.

Privacy verification uses zero-knowledge proof to ensure that sensitive information is not leaked during data transactions [31]. Zero-knowledge proof allows the verifier to confirm the validity of the data without obtaining the data content. The system introduces a zero-knowledge proof protocol to achieve data consistency verification through multiple rounds of interaction. During the data verification process, the prover only shows the ciphertext or related attributes, and the verifier can confirm the legitimacy of the data without decryption, protecting the privacy of information. If transaction verification is performed, the zk-SNARKs (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) scheme is used to generate a short proof for fast verification between nodes. The proof generated by zk-SNARKs is short and convenient, suitable for the efficient distributed storage of blockchain, and reduces the bandwidth required for data verification.

In the compliance scenario of blockchain system, user role permission control is also strengthened through encryption technology. Data access rights are set according to different identity levels, and authorization control is implemented through public and private key mechanisms to ensure that unauthorized users cannot obtain encrypted data. When a user submits a data access request, the system verifies its private key and determines the legitimacy of the request based on the access rights. If it meets the scope of authority, the corresponding access rights are provided by decrypting the relevant data content, achieving hierarchical management of sensitive data access and preventing the risk of sensitive information leakage.

The combination of AES, homomorphic encryption and zero-knowledge proof ensures the security, privacy and compliance of financial data. The solution builds a data privacy protection architecture on the blockchain so that sensitive data is controlled by encryption and verification mechanisms throughout the entire life cycle, reducing the possibility of privacy breaches. Data is always encrypted during transmission, processing and storage, and zero-knowledge proof provides a data consistency verification method to ensure the safety and compliance of the data operation process and ensure the high privacy and security of the on-chain financial system.

## 3.4 Implementation of Financial Data Traceability and Audit Mechanism

The data traceability and audit mechanism of the blockchain system relies on timestamps and tamper-proof features to achieve full tracking of the source and flow of financial data. Based on timestamps, each financial transaction record is given a unique identifier to ensure the accuracy and timeliness of data recorded on the chain. The introduction of timestamps enables transaction serialization, allowing the subsequent data tracking process to be efficiently executed on the chain, ensuring that the tracing process is not interfered with by external factors. The timestamp and transaction record of each piece of data are stored on the chain immediately after they are generated, and the system obtains a complete historical path on the chain. These paths can be used to quickly retrieve the original location of the data during the audit process.

Financial data is organized in a Merkle tree structure to enhance data-tracking accuracy [32]. Merkle tree nodes store the hash value of financial transaction data to ensure that changes within a single node cannot affect the integrity of the entire chain data. The authenticity of the chain data can be verified by the hash value. The unique identifier of the Merkle tree root node is generated by combining the hash values of the data at each level to form a tree structure with consistency and integrity. During the audit process, only the root node needs to be verified to confirm the integrity of the data, which greatly improves the retrieval efficiency. Tampering with any data in the node can cause the hash value to deviate, ensuring that the data on the chain is irreversible.

During the storage of each piece of financial data, the timestamp and transaction ID are associated. This association constitutes a traceable mark for the data on the chain so that the transaction records at any point in time have a complete source and flow tracking path, improving the transparency and compliance of the data. During the audit, the operation records of the upstream nodes are retrieved in reverse according to the timestamp to form a complete transaction history on the chain. For data anomalies in the system, the audit mechanism quickly locates the node through the Merkle tree and its derived path structure to avoid large-scale data backtracking.

Under the multi-node structure in the blockchain network, each node conducts multiple rounds of voting on the validity and consistency of transaction records to prevent inconsistencies in data due to node failures or external interference before being uploaded to the chain, ensuring the integrity and reliability of the uploaded data. The multi-node voting feature of the PBFT consensus mechanism strengthens the tamper-proof ability of on-chain data. The data that is finally uploaded to the chain is derived from the consensus results of multi-node voting, ensuring that the data remains consistent during auditing.

## 3.5 Selection and Optimization of Consensus Algorithm

Given the sensitivity of financial data and the need for multiple nodes on the chain, the PBFT algorithm has become the optimal choice due to its low computing and storage costs [33]. Compared with other consensus algorithms, PBFT can maintain network reliability even when one-third of the nodes fail, thus improving efficiency while ensuring data consistency.

The PBFT algorithm achieves node consistency through a staged voting mechanism. During the voting process, there are three levels, "preparation, preparation, and submission", and the number of records for each level is confirmed after each level is confirmed. During the construction of the PBFT algorithm, the points must be understood to confirm the flow of information, the information must be consistent within a specific time, and the final confirmation of the number of points can be confirmed. Under the current situation, the number of payments is fixed, the voting machine system is reduced in size, the number of guarantees is quickly copied, and the efficiency is high.

To ensure consistency, PBFT operations can increase the system's ability to resist point separation, ensure the independence of the names of the shared reading confirmation time, and reduce the mechanism of common understanding in the middle and the future. Scores, different weights, etc., ensure the sum of numbers is balanced. Threshold signatures prevent malicious scores in the middle of digital changes, and highly distributed formulas have security and digital integrity. When the system is used for voting, the number of PBFT implementation points can be quickly changed to ensure the consistency and security of the system.

The PBFT algorithm uses an asynchronous message-passing architecture in the multi-round consensus process to ensure that the network maintains the stability of the consensus process under high load. During the consensus process, PBFT adopts a mechanism to prevent Byzantine node interference. To ensure data consistency, PBFT uses a prevention mechanism to avoid the potential impact of Byzantine nodes on system performance. The existence of Byzantine nodes cannot interfere with the overall consistency of data writing on the chain. PBFT uses multiple rounds of voting to ensure data equality between each node.

### 3.6 Access Control and Data Sharing Management

The key to ensuring the security and privacy of financial data is to design precise access control and data-sharing management systems on the blockchain platform. Permissions are allocated through the role-based access control (RBAC) mechanism [34], and different roles obtain corresponding data access rights according to their scope of responsibilities. The Fabric identity management module further strengthens the RBAC mechanism, ensuring that each role has access operations within the scope of authority through fine-grained control.

The implementation of the authorized access mechanism depends on the binding of roles and user identities, and Fabric's multi-channel mechanism improves the accuracy of access. The channel access control list (ACL) provides detailed management for data sharing [35], sets access levels based on business needs, and achieves a balance between isolation and sharing among different users. ACL is used in conjunction with RBAC to ensure the transparency and compliance of information flow in multi-user scenarios. The on-chain data flow is recorded in the blockchain's tamper-proof distributed ledger, effectively meeting audit requirements.

For user permission verification and dynamic authorization update, RBAC combines with Fabric chain code to implement real-time verification based on identity and role. When a user requests access, Fabric queries ACL to compare the requested permission level with the access level of the corresponding role to prevent unauthorized access. Fabric chaincode acts as the execution layer for audit records and permission verification during user access, recording each access as an unalterable ledger entry. By using smart contracts to execute permission management, and recording permission allocation and access history on the chain, a transparent permission update link is formed to ensure the fairness and rigor of permission management.

The shared data management mechanism is coordinated with RBAC and the on-chain identity module, allowing the efficient sharing of data between authorized users. In cross-organizational or cross-departmental scenarios, data-sharing can be carried out via specific channels, and RBAC controls access nodes and limits the scope of sharing. Fabric's channel privacy design ensures the isolation of data during sharing and concentrates access rights on specific user groups. Fabric chaincode records all cross-channel sharing operations, and data interactions are recorded in the ledger, achieving comprehensive traceability of data flow and ensuring transparency and compliance of the sharing process.

The RBAC mechanism uses encryption technology to verify user identity and permissions, and saves the encryption results on the chain to achieve two-way verification of identity and data access. After each user registers on the chain, a public and private key pair is generated, and access requests are made with this identity credential. Fabric chain code uses the user's private key signature to match the public key on the chain, and ensures the uniqueness and legitimacy of the access identity through signature verification, eliminating the risk of fake identity. Encryption and on-chain identity authentication are used during data access or sharing to prevent data leakage and ensure secure access.

The optimization of the identity and permission verification process improves the execution efficiency of permission management through the linkage of the RBAC and the chain code. The rules of the fabric chain code automatically execute permission control and identity comparison, reducing manual intervention while ensuring real-time performance. Once the access request is verified, the permission usage is recorded on the chain, the data flow is locked, and the access record is kept for a long time. All on-chain records are processed by chain code hash operations, and user and role information is converted into non-plaintext data storage to ensure that there is no risk of leakage in the data-sharing process.

## 4. EVALUATING THE EFFECTIVENESS OF THE FINANCIAL DATA SECURITY PROTECTION PLAN

### 4.1 Data Security Evaluation

For the evaluation of data security, the traditional symmetric encryption algorithm DES was selected as a comparison object to determine the effect of BT on financial data security.

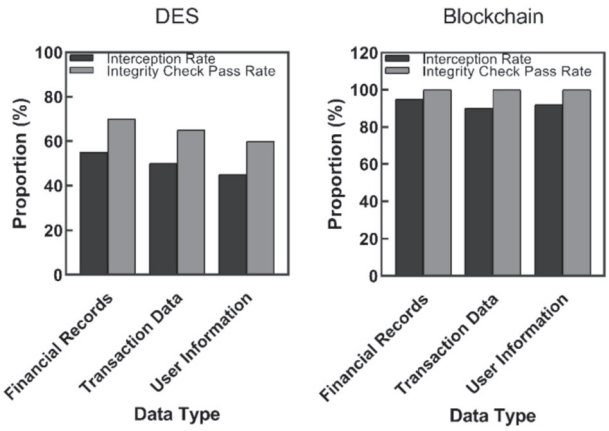


**Figure 4** Results for the experimental interception rate and integrity check pass rate.

**Table 1** Financial Data integrity comparison experimental results.

| Data Type | Encryption Scheme | Tampered Records | Detected Tampering | Tampering Detection Rate (%) | Multi-node Consistency (%) |
|---|---|---|---|---|---|
| Financial Records | MD5 | 5 | 3 | 60 | 85 |
| Financial Records | Blockchain | 5 | 5 | 100 | 100 |
| Transaction Data | MD5 | 5 | 2 | 40 | 80 |
| Transaction Data | Blockchain | 5 | 5 | 100 | 100 |
| User Information | MD5 | 5 | 3 | 60 | 90 |
| User Information | Blockchain | 5 | 5 | 100 | 100 |

In the experiment, the corresponding test environment was designed for different data protection methods to simulate hacker attack scenarios. Finally, the rate of successful interception was calculated.

The test data was divided into two groups: DES encryption was used for one group; and a blockchain-based encryption scheme was used for the other group. Each set of data was subjected to 100 hacker attack simulations to evaluate the encryption strength and integrity protection of the data. When checking the data integrity, the stored data was verified using a hash algorithm to ensure that it had not been tampered with. The DES-based scheme used the SHA-1 hash algorithm for data integrity checks, while the blockchain-based scheme used on-chain records for verification. By comparing the data protection results, the performance of the two schemes in the face of attacks was evaluated.

The experimental results are shown in Figure 4. In regard to the protection of different types of data such as financial records, transaction data, and user information, the interception rate of the blockchain solution is more than 90%, and the integrity check pass rate is 100%. When facing the same number of attacks, the traditional DES encryption solution has a successful interception rate and a data integrity check pass rate of less than 70%. The analysis of the data results shows that the protection solution based on blockchain performs well in terms of data encryption and anti-tampering, and has stronger anti-attack and data protection capabilities.

## 4.2 Financial Data Integrity Assessment

For the assessment of financial data integrity, the traditional MD5 (Message-Digest Algorithm 5) hash algorithm was selected as the comparison object, and a detailed experimental analysis was conducted with the protection scheme based on BT. The performance of the two in actual applications was tested by inserting random data and comparing the recorded hash values.

In the experiment, the same financial data was processed using the MD5 hash algorithm and BT. Ten groups of data were selected, each containing 10 records. In the experiment, 5 records were randomly selected for tampering, and the changes in the hash values were recorded. The tampering detection capability was determined by comparing the untampered and tampered hash values. During the multi-node synchronization process, the consistency of the data of each node was monitored.

Table 1 summarizes the experimental data and results. The experimental results show that the MD5 hash algorithm has a success rate of less than 60% in detecting tampering, while the blockchain solution achieves a 100% detection rate. In terms of multi-node data consistency, the MD5 solution also performs worse than the blockchain solution.

The results show that the blockchain-based protection scheme performs well in terms of financial data integrity protection, which further illustrates the advantages of BT in this field.

## 4.3 Data Privacy Protection Evaluation

For the experimental evaluation of data privacy protection, this study used information leakage rate as the evaluation indicator, selected RSA encryption algorithm and zero-knowledge proof mechanism to encrypt and verify random data, and tested privacy protection performance.

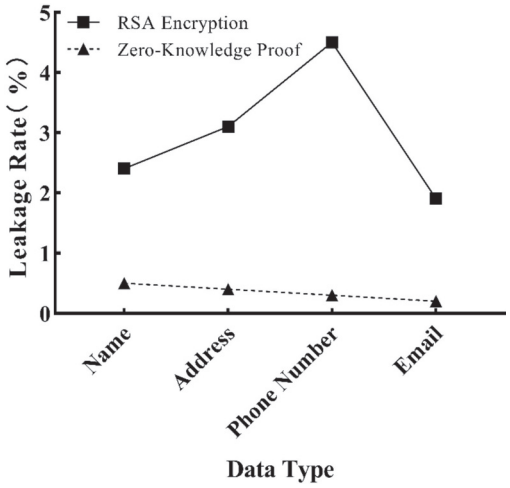


**Figure 5** Privacy protection experiment data.

**Table 2** Data traceability experiment record.

| Operation Type | Blockchain Traceability Time (Seconds) | Centralized Database Traceability Time (Seconds) | Blockchain Consistent Query Count | Centralized Database Consistent Query Count | Total Query Count |
|---|---|---|---|---|---|
| Entry | 0.5 | 2.3 | 500 | 460 | 550 |
| Exit | 0.4 | 2.1 | 480 | 450 | 500 |
| Modification | 0.6 | 2.5 | 520 | 400 | 550 |
| Deletion | 0.5 | 2.4 | 510 | 430 | 550 |
| Query | 0.3 | 1.8 | 490 | 410 | 500 |

For the experiment, 5,000 randomly-generated private data items were used, comprising different sensitive information fields (name, address, phone number, and email). Each record was encrypted in a different way, and the RSA algorithm and the zero-knowledge proof mechanism in BT were compared. In the experiment, the encrypted data was cracked by simulating attacks, and the successful leakage rate of each method was recorded. The experimental results are shown in Figure 5. The privacy protection effect of the zero-knowledge proof mechanism is significantly better than that of RSA encryption. Experimental results showed that the average leakage rate of RSA encryption is about 3%, while the leakage rate of the zero-knowledge proof mechanism is only 0.35%. The results indicate that the use of a blockchain-based privacy protection scheme can significantly improve the security of sensitive data and reduce the risk of information leakage.

## 4.4 Financial Data Traceability and Audit Capability Evaluation

In the experiment conducted to evaluate data traceability and audit capability, a centralized database was selected as the comparison technology. The evaluation indicators used were: traceability time and audit consistency. The experimental design tested the traceability effect in multiple links through the timestamp recording and data tracking function of the blockchain.

The volume of experimental data was set to 2650 records, each of which contains a piece of information for different operations (warehouse entry, warehouse exit, modification, deletion and query). The timestamps and operation records generated by BT were compared with the corresponding records in the traditional database to calculate the traceability time and consistency indicators. The traceability time was determined by measuring the time required from the start of the query to the return of complete traceability information; the audit consistency was evaluated by comparing the returned results of the data under different query conditions. Table 2 presents the experimental data and results.

The experimental results indicate that BT still performs at a superior level in terms of data tracing time. The average tracing time of blockchain is only 0.46 seconds, while the average tracing time of traditional centralized databases is 2.22 seconds. In terms of audit consistency, the audit consistency rate of blockchain is 94.34%, and the audit consistency rate of centralized database is 81.13%. The significant difference between the two evaluation indicators is evidence of the advantages of BT in regard to data consistency, indicating that under the same query conditions, blockchain can provide greater query consistency.

## 4.5 Compliance and Transparency Evaluation

In the experimental design, the traditional relational database (MySQL) was selected as the comparison object. The evaluation indicator is the matching degree between the number of smart contract audit record entries and compliance requirements, which is used to determine whether blockchain technology can improve data-sharing transparency and audit capabilities. In the experiment, data verification was performed through the audit records generated by smart contracts to ensure that the audit entries were consistent with compliance requirements. During the experiment, data

**Table 3** Compliance and transparency evaluation experiment data record.

| Operation Type | Blockchain Audit Record Count | MySQL Database Audit Record Count | Compliance Requirement Count | Blockchain Consistency Verification Rate | MySQL Database Consistency Verification Rate |
|---|---|---|---|---|---|
| Entry | 600 | 550 | 600 | 100.00% | 91.67% |
| Exit | 580 | 520 | 580 | 100.00% | 89.66% |
| Modification | 590 | 500 | 590 | 100.00% | 84.75% |
| Deletion | 610 | 540 | 610 | 100.00% | 88.52% |
| Query | 620 | 560 | 620 | 100.00% | 90.32% |

**Table 4** System anti-attack capability evaluation experimental data record.

| Attack Type | Blockchain Successful Interceptions | Oracle Interceptions | Total Attacks | Blockchain Interception Rate | Oracle Interception Rate |
|---|---|---|---|---|---|
| Denial of Service | 95 | 65 | 100 | 95.00% | 65.00% |
| Data Tampering | 90 | 50 | 100 | 90.00% | 50.00% |
| Malicious Node Invasion | 88 | 40 | 100 | 88.00% | 40.00% |
| Comprehensive Attack (Multiple) | 270 | 155 | 300 | 90.00% | 51.67% |

were collected from different scenarios to compare the audit coverage of the two technologies. Table 3 presents the specific data of the experiment.

From the data in Table 3, it can be seen that the matching degree between the number of audit record entries and compliance requirements of BT has reached 100%, showing extremely high data-sharing transparency. However, the consistency verification rate of MySQL database is significantly lower, at 89% overall. The results indicate that BT still has significant advantages in terms of improving data transparency and compliance.

### 4.6 Evaluation of System Anti-Attack Capability

The system's anti-attack capability is indispensable in modern financial data security protection methods. The traditional centralized database technology (Oracle Database) and the protection solution based on BT are compared to evaluate their performance in terms of attack interception rate and the success of node defense. The evaluation process simulated the attack nodes to test the system's defence of data in actual attack scenarios.

For the experiment, a distributed network fault tolerance test was used to ensure the reliability of the evaluation results. A multi-node blockchain network was constructed to simulate external attacks and record the system's response. Each node was subjected to different types of attacks, including denial-of-service (DoS), data tampering, and malicious node intrusion. According to the attack type, the stability and anti-attack capability of each node was recorded to determine the overall performance of the system. Table 4 shows the experimental data and the performance of traditional databases and BT in different attack scenarios.

The data in Table 4 shows that whether it is a denial-of-service attack, data tampering or malicious node intrusion, the attack-interception rate of the blockchain system is significantly higher than that of the traditional centralized database. After calculation, it is found that the average interception rate of the blockchain system under the four types of attacks is 39.08% higher than that of the traditional centralized database, indicating that BT performs better than the traditional Oracle database in resisting attacks.

## 5. CONCLUSIONS

In response to the risk issues faced by the centralized database structure in the auditing and internal control of traditional financial systems, this study designed a series of innovative methods and algorithms for financial data security protection solutions based on BT. The decentralized storage structure and smart contracts are used to achieve automated management and verification of data, significantly improving the security and credibility of data. In regard to data privacy protection, auditing capabilities and system anti-attack capabilities, experimental results show that BT is superior to traditional centralized databases in all dimensions, especially in terms of the number of attack interceptions and the traceability of financial data. Although this study has achieved some valuable results, the experimental environment is limited by simulation tests and fails to fully cover the complex network conditions in the real world. Future research will explore the effectiveness of the verification method in actual application scenarios, and further explore the optimization algorithm and its application in a wider range of fields, and strive to improve system performance and adaptability to cope with increasingly complex security threats and compliance requirements.

## FUNDING

This work was supported by Fundamental Research Projects of Higher Education Institutions in Liaoning Province, China. Grant: [LJ112411632057]

## REFERENCES


1. Sharma A, Kaur P. Tamper-proof multitenant data storage using blockchain. Peer-to-peer Networking and Applications, 2023, 16(1): 431–449.
2. Yang J, Wen J, Jiang B, et al. Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network, 2020, 34(4): 62–67.
3. Jiachen Yang, Jiabao Wen, Bin Jiang, Huihui Wang. Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization, 2019, 29(2): 105–117.
4. Mosteanu N R, Faccia A. Digital systems and new challenges of financial management–FinTech, XBRL, blockchain and cryptocurrencies. Quality–Access to Success, 2020, 21(174): 159–166.
5. Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. De Paula, Natasha Malara Borges. Developing a global data breach database and the challenges encountered. Journal of Data and Information Quality (JDIQ), 2021, 13(1): 1–33.
6. Abrera J. Data Privacy and Security in Cloud Computing: A Comprehensive Review. Journal of Computer Science and Information Technology, 2024, 1(1): 01–09.
7. Zachariadis M, Hileman G, Scott S V. Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization, 2019, 29(2): 105–117.
8. Demirkan S, Demirkan I, McKee A. Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 2020, 7(2): 189–208.
9. Liu Y, Zhang J, Zhan J. Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Computing, 2021, 24(2): 1331–1345.
10. Da Xu L, Lu Y, Li L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 2021, 8(13): 10452–10473.
11. Liu R, Wang E. Blockchain and mobile client privacy protection in e-commerce consumer shopping tendency identification application. Soft Computing, 2023, 27(9): 6019–6031.
12. Lohith Paripati, Nitin Prasad, Jigar Shah, Narendra Narukulla, Venudhar Rao Hajari. Blockchain-enabled data analytics for ensuring data integrity and trust in AI systems. International Journal of Computer Science and Engineering (IJCSE), 2021, 10(2): 27–38.
13. Maariz A, Wiputra M A, Armanto M R D. Blockchain technology: Revolutionizing data integrity and security in digital environments. International Transactions on Education Technology (ITEE), 2024, 2(2): 92–98.
14. Namperumal G, Sivathapandi P, Venkatachalam D. The Role of Blockchain Technology in Enhancing Data Integrity and Transparency in Cloud-Based Human Capital Management Solutions. Journal of Artificial Intelligence Research and Applications, 2023, 3(1): 546–582.
15. Tatineni S. Blockchain and Data Science Integration for Secure and Transparent Data Sharing. International Journal of Advanced Research in Engineering and Technology (IJARET), 2019, 10(3): 470–480.
16. Chen X, Tang Y. Data center energy management based on cloud computing and artificial intelligence[J]. Engineering Intelligent Systems, 2024, 32(3): 257–266.
17. Olubusola Odeyemi, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, Omotayo Bukola Adeoye, Wilhelmina Afua Addy, Adeola Olusola Ajayi-Nifise. Integrating AI with blockchain for enhanced financial services security. Finance & Accounting Research Journal, 2024, 6(3): 271–287.
18. Jimmy F. Enhancing Data Security in Financial Institutions with Blockchain Technology. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006–4023, 2024, 5(1): 424–437.
19. Li Zhang, Yongping Xie, Yang Zheng, Wei Xue, Xianrong Zheng, Xiaobo Xu. The challenges and countermeasures of blockchain in finance and economics. Systems Research and Behavioral Science, 2020, 37(4): 691–698.
20. Rijanto A. Blockchain technology adoption in supply chain finance. Journal of Theoretical and Applied Electronic Commerce Research, 2021, 16(7): 3078–3098.
21. Lingling Guo, Jingjing Chen, Shihan Li, Yafei Li, Jinzhi Lu. A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance. Digital Communications and Networks, 2022, 8(4): 576–587.
22. Mustyala A. Leveraging Blockchain for Fraud Risk Reduction in Fintech: Infrastructure Setup and Migration Strategies. EPH-International Journal of Science and Engineering, 2023, 9(2): 1–10.
23. George A S. Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. Partners Universal Innovative Research Publication, 2023, 1(1): 54–66.
24. Becherer M, Zipperle M, Hussain O K, den Hartog F, Zhang Y, Chang E, et al. Enabling Trustworthy Collaboration for Sustainable Transformation[J]. Engineering Intelligent Systems, 2024, 31(1): 43–51.
25. Melo C, Oliveira F, Dantas J, et al. Performance and availability evaluation of the blockchain platform hyperledger fabric. The Journal of Supercomputing, 2022, 78(10): 12505–12527.
26. Lu Z, Mohamed H. A complex encryption system design implemented by AES. Journal of Information Security, 2021, 12(2): 177–187.
27. Alenezi M N, Alabdulrazzaq H, Mohammad N Q. Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 2020, 12(2): 256–272.
28. Attkan A, Ranga V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence-based key-security. Complex & Intelligent Systems, 2022, 8(4): 3559–3591.
29. Cheqing Jin, Shuaifeng Pang, Xiaodong Qi, Zhao Zhang, Aoying Zhou. A high-performance concurrency protocol for smart contracts of permissioned blockchain. IEEE Transactions on Knowledge and Data Engineering, 2021, 34(11): 5070–5083.
30. X. Ma, Y. Zhang, "Blockchain Data Privacy Protection Mechanism for Enterprise Finance and Data Mining Algorithms", Engineering Intelligent Systems, vol. 32 no. 5, pp. 435–443, 2024.
31. Wan Z, Zhou Y, Ren K. Zk-AuthFeed: Protecting data feed to smart contracts with authenticated zero knowledge proof. IEEE Transactions on Dependable and Secure Computing, 2022, 20(2): 1335–1347.
32. Junlu Wang, Su Li, Ji Wanting, Dong Li, Baoyan Song. A composite blockchain associated event traceability method for financial activities. Peer-to-Peer Networking and Applications, 2023, 16(4): 1696–1715.
33. Jinyu Zhang, Yumeng Yang, Deyu Zhao, Yue Wang. A node selection algorithm with a genetic method based on PBFT in consortium blockchains. Complex & Intelligent Systems, 2023, 9(3): 3085–3105.
34. Y. Gao, L. Sun, "Credit Risk Evaluation of Science and Technology Finance Based on Artificial Intelligence and

Bayesian Algorithm", Engineering Intelligent Systems, vol. 32 no. 5, pp. 445–455, 2024.
35. Raj S, Kumar B A, Venkatesan G K D. A security-attribute-based access control along with user revocation for shared data in multi-owner cloud system. Information Security Journal: A Global Perspective, 2021, 30(6): 309–324.

**Su Meng** was born in Shenyang, Liaoning. P.R. China, in 1989. She received the master's degree from Liaoning University, P.R. China. Currently, she is working at the Shenyang Institute of Engineering. Her research interests include finance, auditing, internal control, information security and big data analysis.