Privacy Protection and Management in Logistics Supply Chains Based on Blockchain Technology and Encryption Algorithms

Ying Chen[1,*], Xiaojuan Yue[2] and Wang Pan[1]

[1]*Jiangsu Aviation Technical College, Zhenjiang, Jiangsu, China*
[2]*Chongqing Finance and Economics College, Chongqing, China*
E-mail: chenying@jatc.edu.cn
[*]*Corresponding Author*

Received 10 November 2025; Accepted 11 December 2025

Abstract

To deal with the issues of data privacy leakage and low collaborative management efficiency in the digitalization of logistics supply chains, this study proposes a privacy protection method integrating blockchain technology and attribute-based encryption, along with a multi-blockchain collaborative management system. The method achieves Fine-Grained Access Control (FGAC) and secure sharing of logistics data through a hierarchical blockchain architecture and an attribute-based encryption mechanism supporting dynamic revocation. The system adopts a dual-chain model with a logistics mainchain and a regulatory blockchain, utilizing smart contracts for business execution and audit supervision collaboration. Results show that under 35 attribute conditions, encryption and decryption times are 41.5 ms and 33.0 ms respectively, outperforming comparative algorithms. For a 64 MB file, encryption and decryption times are 234.1 ms and 199.1 ms. In high-concurrency scenarios, the system achieves read and write throughput rates of 342 TPS and 252 TPS. The proposed system demonstrates a throughput of 449 TPS under high

Journal of Cyber Security and Mobility, Vol. 14_6, 1475–1504.
doi: 10.13052/jcsm2245-1439.1467

load, with transaction confirmation latency of 116.9 ms. Data compression ratio reaches 39.8%, audit accuracy improves to 98.7%, and cross-chain transaction success rate reaches 97.6%. The research results indicate that the designed system exhibits significant merits in privacy protection, processing efficiency, and cross-chain collaboration. Its core security advantage stems from the fine-grained dynamic revocable access control implemented by CP-ABE technology, which effectively curbs unauthorized data access. At the same time, it adopts an elastic dual-chain architecture reinforced by a node rotation mechanism based on verifiable random functions, which can resist collusion attacks and 51% attacks by regulators. This provides an effective solution for building a trusted and efficient digital logistics supply chain.

Keywords: Blockchain, attribute-based encryption, logistics supply chain, privacy protection, data security.

1 Introduction

With the continuous expansion of global trade and the advancement of e-commerce, modern Logistics Supply Chain (LSC) systems are becoming increasingly complex, networked, and digitized [1]. Massive data frequently flows between multiple parties, covering key processes such as orders, warehousing, transportation, and delivery. However, the high degree of data sharing and collaboration also brings serious privacy and security challenges [2]. Logistics data contains sensitive business information that may be accessed or leaked without authorization during transmission or storage. This can lead to significant business losses and reputational risks [3]. The traditional centralized data management model is difficult to effectively solve the growing problems of data tampering, information silos, and privacy violations due to its single point of failure, lack of transparency, and excessive reliance on third-party organizations [4]. In recent years, Blockchain Technology (BT) has emerged as a promising solution. BT ensures the integrity and authenticity of data by recording transaction and logistics information in a blockchain format. This information is synchronized and verified across all network nodes through consensus mechanisms [5].

With its decentralized, tamper-proof, traceable and transparent characteristics, BT provides a revolutionary solution for building a trustworthy and secure Supply Chain (SC) management system. Wei Q. et al. investigated the issue of limited research into blockchain data management systems, focusing on three common types of blockchain. This study analyzed the

data management mechanism across three layers: blockchain architecture, data structure and storage engine. The findings denoted that there were still technical challenges in the management mechanisms of various layers of blockchain data management [7]. Gudala L et al. proposed a data enhanced security method that integrates biometric recognition and blockchain, which stores encrypted biometric hashes in a distributed ledger and automatically executes access control using smart contracts. The results indicated that this method could improve data tamper resistance and user privacy control [8]. Das D et al. proposed an intelligent transportation data management system based on blockchain and smart contracts. The system automatically verified vehicle data and charged fees by deploying smart contracts, and designed effective data verification algorithms. It was found that the system could improve data security and user privacy [9]. Yang C et al. designed a quality management platform supported by edge cloud blockchain and the IoT to address the difficulties in quality management and low data transparency in SC logistics. This platform utilized mobile and fixed edge gateways and synchronization engines to ensure data integrity. The findings denoted that the platform could achieve data collection and effectively improve the level of quality management [10].

However, due to the inherent data openness or semi openness of blockchain, directly uploading sensitive data to the chain will face serious privacy leakage risks. In this context, advanced Encryption Algorithms (EAs) have become a key technological means to balance blockchain transparency and data privacy [11]. Ping J et al. developed a blockchain-based privacy protection optimization method to address the vulnerability and privacy leakage issues of traditional solutions in peer-to-peer energy trading. This method submitted transaction information through EAs and coordinates privacy protection with Byzantine fault-tolerant algorithms. The findings denoted that this method could effectively protect privacy and resist dishonest behavior [12]. Jiang Y et al. proposed an electronic health record protection scheme that combines BT with Attribute-Based Encryption (ABE). By storing encrypted data in the form of transactions on the blockchain, the scheme ensured data integrity and controllable access. As a result, it was found that the computational cost of this scheme decreased by a maximum of 5.2% [13]. Wan et al. suggested an efficient, scalable blockchain consensus algorithm that conceals the leader node's identity using EAs, and employs one-to-many communication to minimise the complexity of messages. The findings denoted that the algorithm could improve throughput by 49.3% while ensuring security [14]. Zhang K et al. suggested a data sharing scheme

Table 1 Comparative analysis of existing blockchain-based privacy protection studies

References	Core Contribution	Key Limitations in Logistics Scenarios
[7]	Survey of blockchain data management systems	Lacks specific solutions for dynamic permission management in multi-party logistics operations
[8]	Biometric-blockchain integration for access control	Static authentication unsuitable for frequent role changes in SCs
[9]	Blockchain-based transportation management system	No support for fine-grained attribute revocation in logistics workflows
[10]	Edge-cloud blockchain for quality management	Limited cross-chain capability hindering regulatory-compliance collaboration
[12]	Privacy-preserving energy trading optimization	Single-chain architecture insufficient for complex logistics business segregation
[13]	EHR protection with ABE and blockchain	Lacks multi-chain collaborative mechanism for logistics audit and execution
[14]	Efficient blockchain consensus algorithm	No consideration for dual-chain interoperability in SC contexts
[15]	Blockchain-based encrypted data sharing	Limited support for real-time permission updates in dynamic logistics environments

grounded on blockchain and encrypted search algorithms. This scheme achieved tamper proof and integrity verification by hiding access policy attributes and storing secure indexes in the blockchain and ciphertext in the file system. The findings denoted that the scheme was safe and effective, and had practical value [15]. To critically analyze the applicability of existing research in logistics scenarios, a comparison of their shortcomings in key areas is provided in Table 1.

There have been studies exploring the application of blockchain in the SC. However, the existing single blockchain architecture is difficult to carry the complex business of the entire chain, and the privacy protection mechanism has not effectively integrated the dynamic ABE scheme that supports security attribute revocation, which cannot meet the practical needs of frequent changes in the roles and permissions of logistics participants [16]. In view of this, an LSC privacy protection method based on BT and EAs is proposed, and a multi-blockchain collaborative Logistics Supply Chain Management System (LSCMS) is designed to strengthen the privacy protection capability of the LSC, while achieving more efficient and secure data sharing and management. The novelty of this study lies in the integration of ciphertext policy ABE with blockchain to achieve attribute-based access control of

logistics data, and the automatic anchoring and audit triggering between the two chains through smart contracts to achieve collaboration between core business execution and compliance supervision.

2 Methodology

A LSC privacy protection method combining blockchain and ABE algorithm is proposed, and an LSCMS based on multi-blockchain collaboration is designed to enhance the scalability, regulatory transparency, and overall operational efficiency of the system.

2.1 Privacy Protection Method for LSC Combining Blockchain and ABE Algorithm

With the continuous improvement of digitalization in LSC systems, data sharing and collaboration among multiple participants have become the norm [17]. Although BT has advantages such as decentralization, immutability, and traceability, its data openness also brings potential risks of privacy breaches [18]. ABE, as an encryption mechanism that supports Fine-Grained Access Control (FGAC), can dynamically control data access permissions grounded on user attributes [19]. Therefore, this study proposes a privacy protection method for LSCs that integrates blockchain and ABE algorithms. The aim is to achieve FGAC and secure sharing of logistics data. The study first constructs a layered blockchain architecture for privacy protection in LSCs, achieving decoupling of data collection and transmission, logistics transactions, and data applications. The schematic diagram of its architecture is denoted in Figure 1.

In Figure 1, the blockchain architecture for privacy protection in LSC is divided into data collection and transmission layer, blockchain layer, and data application layer. The data collection and transmission layer is responsible for collecting logistics data and transmitting it; The blockchain layer is responsible for executing logistics transactions and recording circulation status; The data application layer provides interfaces for identity registration, customer and enterprise queries, etc. The study uses mathematical construction based on bilinear pairs to generate the necessary master key and common parameters for system operation, as shown in Equation (1).

$$\begin{cases} \mathrm{PK} = (g, h = g^{\beta}, e(g,g)^{\alpha}) \\ \mathrm{MK} = (\beta, g^{\alpha}) \end{cases} \tag{1}$$

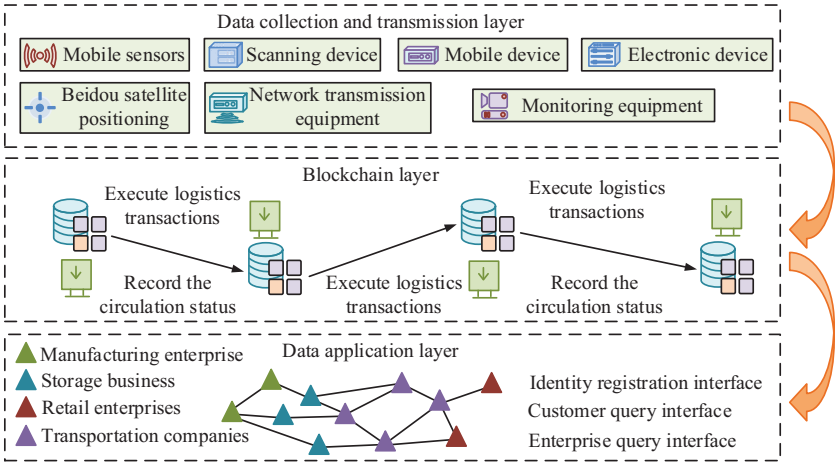


Figure 1 Schematic diagram of blockchain architecture for privacy protection in LSC.

In Equation (1), PK represents the public key; MK represents the master key; g represents the generator of the cyclic group; $h = g^{\beta}$ represents the public key portion calculated from the generator g and the random number; $e(g,g)^{\alpha}$ represents the result of bilinear mapping, where e is a bilinear pairwise mapping and α is a randomly selected privacy index; β represents a randomly selected secret value; g^{α} represents the secret value calculated from the generator g and the random number α. In the attribute key generation stage, it is necessary to generate a private key corresponding to each user's attribute set, as shown in Equation (2).

$$\mathrm{SK} = (D = g^{(\alpha+\gamma)/\beta}, \forall_j \in S : D_j = g^{\gamma} \cdot G(j)^{\gamma_j}, D'_j = g^{\gamma_j}) \tag{2}$$

In Equation (2), SK represents the user's private key; γ represents a random number selected by a trusted institution for the user; S represents the set of user attributes; j represents the attributes in the attribute set; γ_j represents an integer randomly selected for each attribute j; D represents the main component of the private key; D_j and D'_j respectively represent the key components 1 and 2 of attribute j. In this system, the functions of the "trusted institution" are implemented in a decentralized manner through key management service smart contracts deployed on the blockchain. The master key is distributed to multiple permissioned nodes (such as core logistics enterprises or regulators) via a threshold secret sharing scheme, rather than being controlled by a single entity. System initialization and key generation require collaborative execution by a quorum of nodes. When users request private

keys, a threshold subset of nodes use their respective key shares to generate partial components, which are ultimately assembled into a complete private key by the smart contract. This design ensures that no single node possesses the full master key, fundamentally eliminating the single point of failure risk of key leakage. Key management is designed as an infrequent operation, with computational load distributed across nodes. Routine data encryption and decryption are performed locally by users and do not consume blockchain network resources. This distributed architecture maintains the decentralized nature of blockchain while ensuring the security and performance of key management. When data owners wish to share logistics data, they need to encrypt the data according to pre-set access policies [20]. The encryption process combines the efficiency of symmetric encryption with the flexible access control of ABE, and uses the ABE algorithm based on ciphertext policy to encrypt the symmetric key, as shown in Equation (3).

$$\begin{aligned} \mathrm{CT} = (T, \tilde{C} = M \cdot e(g,g)^{\alpha s}, C = h^s, \forall\, y \in Y : C_y = g^{q_y(0)}, \\ C'_y = H(\mathrm{att}(y))^{q_y(0)}) \end{aligned} \tag{3}$$

In Equation (3), CT represents the generation of ciphertext; T represents the access policy tree structure; M represents the actual symmetric key to be encrypted; s represents the secret value of the root node; y represents accessing a leaf node in the tree; $\mathrm{att}(y)$ means the attribute corresponding to leaf node y; $q_y(0)$ represents the value of the secret shared polynomial at point 0 at node y; $\tilde{C}$ and C respectively represent the encrypted symmetric key and system level ciphertext component; C_y and C'_y respectively represent the attribute level ciphertext components corresponding to each attribute in the access policy. After obtaining the ciphertext, the authorized user initiates the decryption process, which is calculated as shown in Equation (4).

$$F_y = (e(D_i, C_y)/e(D'_i, C'_y)) = e(g,g)^{\gamma q_y(0)} \tag{4}$$

In Equation (4), F_y represents the decryption result of leaf node y; i represents the attribute corresponding to leaf node y. Then, the computation recursively proceeds upward until reaching the root node. The final decryption calculation is shown in Equation (5).

$$\begin{cases} F_R = e(g,g)^{\gamma s} \\ \tilde{C}/(e(C,D)/F_R) = M \end{cases} \tag{5}$$

In Equation (5), F_R represents the decryption result at the root node; M represents the original message obtained after decryption. To ensure forward

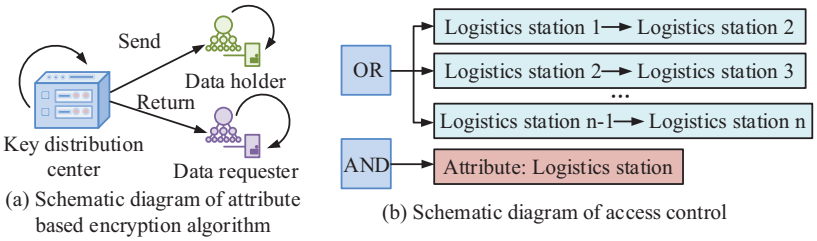
and backward security during dynamic attribute updates, a re-encryption mechanism is implemented upon attribute revocation. When a user's attribute is revoked, the system generates a new random secret value and updates the affected ciphertexts as shown in Equation (6).

$$\begin{cases} C_0' = C_0 \cdot e(g,g)^{\alpha s'} \\ C_1' = g^{s'} \end{cases} \tag{6}$$

In Equation (6), C_0' and C_0 respectively represent the new message encapsulation part after re encryption and the message encapsulation part in the original ciphertext; C_1' represents the encrypted ciphertext component after re encryption; s' represents the new random secret index generated during the re encryption process. This process ensures that users who no longer satisfy the access policy cannot decrypt future data (forward security) and also lose access to previously encrypted data (backward security). The re-encryption is triggered automatically via a smart contract, which also records the revocation event and the updated ciphertext identifiers on the blockchain for auditability.

To handle key conflicts during concurrent access by multiple users, a ciphertext versioning mechanism is employed. Each ciphertext is associated with a version ID that is incremented upon re-encryption. The smart contract enforces a first-commit-wins policy for concurrent updates, using the transaction timestamp and block confirmation order to resolve conflicts. User key states and attribute sets are updated atomically via the smart contract to ensure consistency across the system. To ensure the immutability and traceability of access policies, it is necessary to construct these information into transactions and store them on the blockchain. The schematic diagram of ABE algorithm and access control is denoted in Figure 2.

In Figure 2(a), the data holder distributes keys to data requesters who meet the attribute requirements through a key distribution center. After obtaining



(a) Schematic diagram of attribute based encryption algorithm

(b) Schematic diagram of access control

Figure 2 Schematic diagram of ABE algorithm and access control.

Table 2 Pseudocode table

Pseudocode for Attribute Revocation Smart Contract

FUNCTION handleAttributeRevocation(revokedUserId, revokedAttribute)
// 1. Verify the identity and authority of the revoker
IF !isAuthorizedRevoker(msg.sender) THEN REVERT
 	
// 2. Record the revocation event on-chain
LOG Event RevocationRecorded(revokedUserId, revokedAttribute, block.timestamp)
 	
// 3. Retrieve list of data identifiers (e.g., Ciphertext IDs) associated with the revoked attribute
affectedCiphertexts = getAffectedCiphertexts(revokedAttribute)
 	
// 4. For each affected ciphertext, trigger the re-encryption process
FOR EACH ciphertextId IN affectedCiphertexts DO
// a. Fetch the current ciphertext CT from off-chain storage
currentCT = getCiphertextFromStorage(ciphertextId)
 	
// b. Generate a new random secret value s'
new_s = generateRandomSecret()
 	
// c. Perform re-encryption to produce new ciphertext CT'
newCT = reEncrypt(currentCT, new_s) // Implements Equation (6)
 	
// d. Update the ciphertext record in off-chain storage
updateCiphertextInStorage(ciphertextId, newCT)
 	
// e. Emit event for off-chain listeners (e.g., applications, users)
LOG Event CiphertextUpdated(ciphertextId, newCT)
END FOR
 	
// 5. Update the user's key state or attribute set to reflect the revocation
updateUserAttributes(revokedUserId, revokedAttribute, "REVOKED")
END FUNCTION

the key, the requester can request data from the holder to achieve FGAC; Figure 2(b) constructs a logical access policy that allows data requesters to successfully decrypt and access data when their attributes meet the preset full path policy. The following pseudocode exemplifies the core logic executed by the smart contract upon a revocation event, as shown in Table 2.

2.2 LSCMS Based on Multi-blockchain Collaboration

The proposed privacy protection methods for LSCs have made some progress in data access control and dynamic permission management. However, in

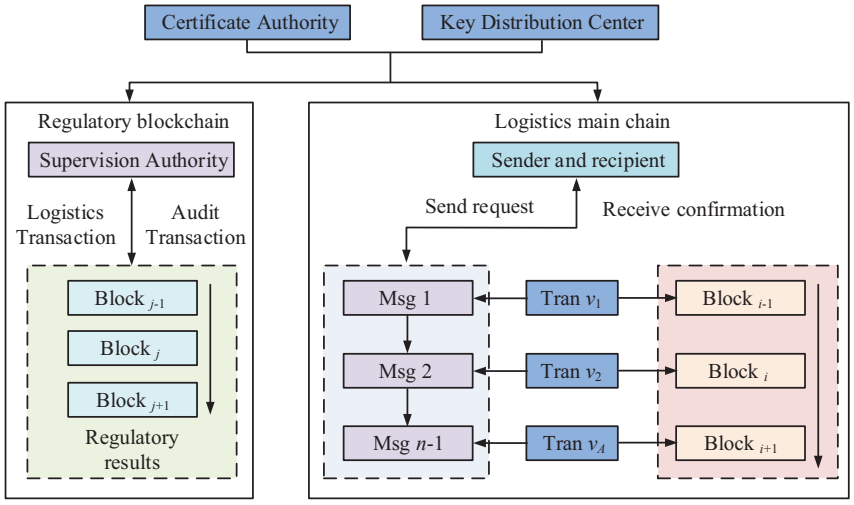


Figure 3 LSCMS based on multi-blockchain collaboration.

actual LSCs, a single blockchain architecture is difficult to support complex multi-party collaboration and management requirements [21]. Therefore, an LSCMS based on multi-blockchain collaboration is proposed to improve the scalability, regulatory transparency, and cross chain collaboration efficiency of the system. The system adopts a dual chain architecture, including a logistics main chain and a regulatory blockchain, respectively responsible for logistics transaction execution and regulatory audit tasks. The schematic diagram of its overall architecture is denoted in Figure 3.

In Figure 3, the core of the LSCMS consists of a logistics main chain and a regulatory blockchain. The logistics main chain is responsible for processing core logistics transactions, which are packaged into blocks and recorded in a chain after confirmation; Regulatory blockchain specialists conduct audit supervision, and regulatory agencies initiate audit requests for specific transactions on the logistics main chain. In the operation of the management system, each participant registers their identity in the system and is assigned a unique identity identifier and initial key pair by the management agency [22]. The registration information is recorded in the regulatory blockchain, and the transaction is packaged into a block after being confirmed by the logistics site, as shown in Equation (7).

$$\begin{cases} \mathrm{RegTx} = \{\mathrm{ID}, \mathrm{PK}_{\mathrm{user}}, \mathrm{TS}, \mathrm{Sig}_{\mathrm{reg}}\} \\ \mathrm{TranA} = \{\mathrm{OderID}, \mathrm{CT}_{\mathrm{data}}, P, H_{\mathrm{prev}}\} \end{cases} \tag{7}$$

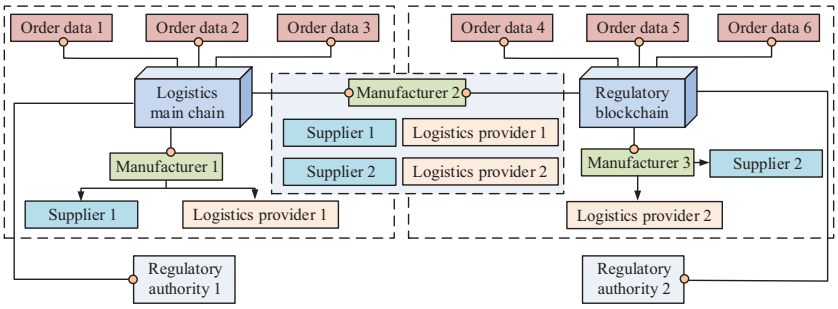


Figure 4 Schematic diagram of hierarchical blockchain architecture.

In Equation (7), RegTx represents registered transactions; ID stands for identity identifier; $\mathrm{PK_{user}}$ represents the user's public key; TS stands for timestamp; $\mathrm{Sig_{reg}}$ represents the signature of the management agency; TranA represents logistics transactions; OderID represents the order identifier; $\mathrm{CT_{data}}$ represents ciphertext data; P stands for access policy; H_{prev} represents the hash value of the previous block. When logistics transactions involve sensitive operations, the management agency audits the request, generates regulatory transactions, and writes them into the management blockchain, as shown in Equation (8).

$$\begin{cases} \mathrm{Req_{super}} = \{\mathrm{TranA_{ID}}, P_{\mathrm{audit}}, \mathrm{TS}\} \\ \mathrm{SuperTx} = \{\mathrm{Req_{ID}}, R, \mathrm{Sig_{super}}\} \end{cases} \tag{8}$$

In Equation (8), $\mathrm{Req_{super}}$ represents management request; $\mathrm{TranA_{ID}}$ stands for logistics transaction identifier; P_{audit} stands for audit strategy; $\mathrm{SuperTx}$ stands for managing transactions; $\mathrm{Req_{ID}}$ stands for request identifier; R represents the audit result; $\mathrm{Sig_{super}}$ represents the signature of regulatory agencies. The LSCMS based on multi-blockchain collaboration adopts a hierarchical blockchain architecture, as shown in Figure 4.

In Figure 4, the hierarchical blockchain architecture achieves collaborative operation between dual chains through smart contracts. The logistics main chain, as the core of the business, is responsible for recording the complete logistics transaction process from order data; Regulatory oversight of blockchain conducts audit supervision over critical transactions and operations on the main chain. The study adopts a dual hashing mechanism to ensure strong correlation between blocks, as shown in Equation (9) [23].

$$\mathrm{Hash}_{b_u} = H(H(\mathrm{header}_{u-1}) \| H(Tx_u) \| \mathrm{Nonce}) \tag{9}$$

In Equation (9), Hash_{b_u} denotes the hash value of the uth block; H stands for cryptographic hash function; header_{u-1} denotes the header information of the previous block; Tx_u means all transaction sets contained in the current block; Nonce stands for random number. When transactions on the logistics main chain need to undergo management audits, the system calculates the Merkle tree root hash of the transaction data and anchors it to the regulatory chain, as shown in Equation (10) [24].

$$\mathrm{MR} = \mathrm{MT}(H(Tx_1), H(Tx_2), \ldots, H(Tx_n)) \tag{10}$$

In Equation (10), MR represents the root hash of the Merkle tree; MT represents the function for constructing Merkle trees; $H(Tx_1), H(Tx_2), \ldots, H(Tx_n)$ denotes the hash value sequence of a single transaction. The system automatically monitors logistics transactions through smart contracts and triggers management audits when any of the following conditions are met, as shown in Equation (11).

$$T_{\mathrm{audit}} = \begin{cases} \text{True if } \mathrm{Value}_{tx} \geq \theta_{\mathrm{value}} \\ \text{True if } \exists\ \mathrm{Risk}_{\mathrm{pattern}}(Tx_u) \\ \text{True if } T_d \geq \theta_t \end{cases} \tag{11}$$

In Equation (11), T_{audit} represents the regulatory audit trigger signal; Value_{tx} and θ_{value} respectively represent transaction amount and transaction amount threshold; $\mathrm{Risk}_{\mathrm{pattern}}(Tx_u)$ stands for risk pattern recognition function; T_d represents delay time; θ_t represents the timeliness threshold. To rigorously assess the security of the dual-chain architecture, an attack tree analysis was conducted, identifying potential threats such as transaction forgery on the main chain and, critically, 51% attacks aimed at tampering with audit data on the regulatory blockchain. A primary concern is an attacker gaining majority control over the regulatory chain's consensus nodes to alter or falsify audit records. To mitigate such colluding attacks, a consensus node rotation mechanism was implemented for the regulatory blockchain. This scheme operates as follows: The set of active consensus nodes is not static but is periodically updated based on a verifiable random function and the nodes' accumulated reputation score. This rotation occurs at random intervals within a predefined window, making it unpredictable for potential attackers. The process for selecting new nodes prioritizes those with high reputation scores and low historical collaboration, thereby increasing the resource cost and coordination complexity required to launch a sustained 51% attack. This dynamic reconfiguration enhances the system's resilience against targeted

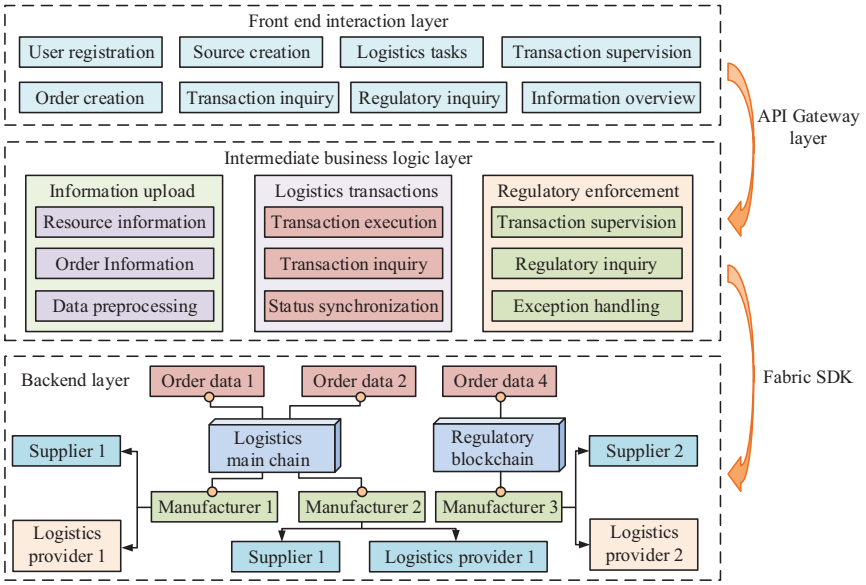


Figure 5 Schematic diagram of LSCMS.

joint attacks on the regulatory layer. The system updates its reputation score dynamically based on the historical behaviour of nodes [25]. The reputation evaluation is shown in Equation (12).

$$\mathrm{TS}_i = a \cdot \frac{N_h}{N_t} + b \cdot \sum_{\Delta t} \frac{T_r}{\Delta t} + c \cdot C_{y_i} \tag{12}$$

In Equation (12), TS_i indicates the reputation score of node i; N_h and N_t respectively represent amount of honest transactions and the total amount of transactions; T_r represents response time; Δt represents a time window or interval; C_{y_i} represents the data consistency index of node i; a, b, and c represent weight coefficients. The schematic diagram of the LSCMS is denoted in Figure 5.

Figure 5 showcases the overall architecture of an LSCMS based on multiple blockchains. The front-end interaction layer serves as the user interface, providing functions such as user registration, order creation, logistics task execution, and transaction supervision, supporting information uploading, querying, and status tracking. The back-end layer, as the core of the system, integrates the logistics main chain and regulatory blockchain. Regulatory blockchain operates in parallel, responsible for regulatory queries and

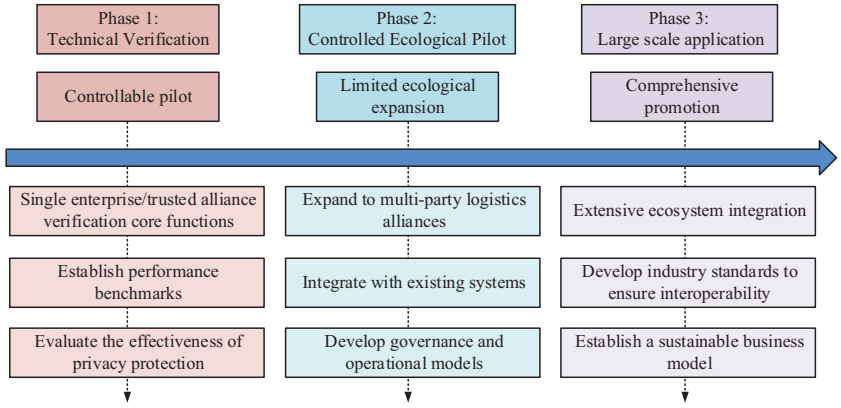


Figure 6 Logistics blockchain system deployment roadmap.

compliance audits, achieving separation and collaboration between business and regulation.

A phased deployment roadmap is proposed to transition the system from laboratory validation to industrial application. As shown in Figure 6. This roadmap emphasizes a phased and gradual strategy to ensure that the technical and operational challenges of each stage are fully addressed, providing a clear path for the system to smoothly transition from an experimental environment to mature industrial applications.

3 Results and Analysis

The effectiveness of the proposed LSC privacy protection method is analyzed to validate its efficiency in encryption/decryption and latency. Subsequently, the effectiveness of the LSCMS is tested to evaluate its reliability under high-concurrency scenarios.

3.1 Performance Analysis of Privacy Protection Methods for LSC

To verify the effect of the proposed LSC privacy protection method based on blockchain and ABE, a simulation experimental environment was built and compared with various mainstream EAs. The experiment used Hyperledger Fabric 2.5 as the blockchain platform. The Fabric network was configured with four sorting nodes, which use Kafka consensus mechanism to form a Kafka based sorting service cluster to ensure fault tolerance and complete orderliness of transactions. As shown in Figure 7, the network topology

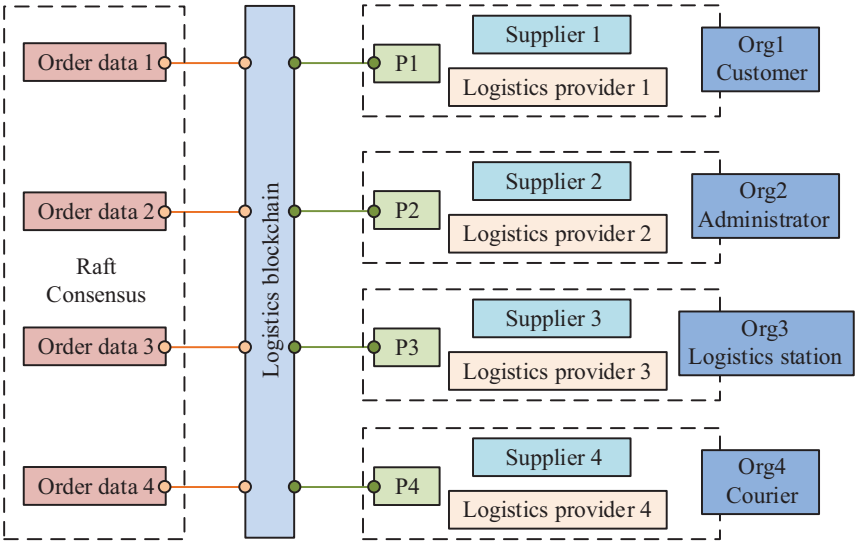


Figure 7 Schematic diagram of the network structure of logistics blockchain.

consisted of four organizations (Org1–Org4), representing different roles of participants in the logistics ecosystem (customers, administrators, logistics sites, couriers). Each organization maintained a peer node (P1–P4) and could configure additional nodes as needed to achieve high availability. These nodes were distributed in simulated geographical areas to reproduce the real network environment. All peer nodes communicated with the central sorting service cluster to complete transaction sorting and block distribution. The experimental environments were: Intel Xeon Silver 4210 CPU, 64 GB RAM, 1 TB SSD, and Ubuntu 20.04 LTS operating system. The experimental hardware configuration was selected to provide a stable and high-performance baseline for evaluating the proposed system's capabilities under demanding conditions, rather than representing a typical deployment scenario. It was acknowledged that the CPU core count (10 cores/20 threads in this case) and network bandwidth (1 Gbps in our lab setup) could influence performance, particularly throughput and latency under high concurrency. The dataset for simulation was generated to reflect typical LSC operations, comprising 100,000 synthetic logistics transaction records. The total simulation data size was approximately 64 GB. The attribute distribution for the ABE scheme was designed with 35 distinct attributes, covering roles, data sensitivity levels, and regional permissions, to test FGAC under realistic conditions. Comparative EAs included Rivest Shamir Adleman (RSA) algorithm, Cipher Policy ABE

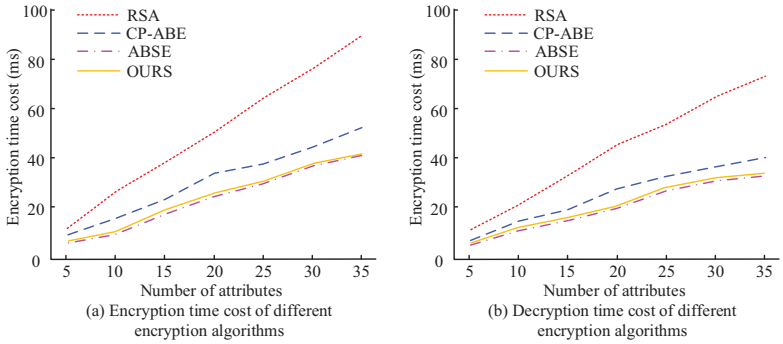


Figure 8 The encryption and decryption time cost of different EAs under different attribute quantities.

(CP-ABE) algorithm, and Attribute-Based Searchable Encryption (ABSE) algorithm. Among them, the implementation of RSA algorithm adopted a key length of 2048 bits. The CP-ABE algorithm was implemented using CP-ABE Toolkit 1.0. The ABSE algorithm was implemented according to the scheme in reference [15] and adopted the same security level.

The study first compared and analyzed the encryption and decryption time costs of different EAs under different attribute quantities, and the findings are denoted in Figure 8. In Figure 8(a), when the amount of attributes was 5, the encryption time costs of RSA, CP-ABE, ABSE, and the proposed algorithm were 12.5 ms, 8.2 ms, 6.8 ms, and 7.5 ms, respectively. When the amount of attributes increased to 35, the encryption time costs of the four algorithms were 88.4 ms, 49.8 ms, 41.2 ms, and 41.5 ms, respectively. In Figure 8(b), when the amount of attributes was 5, the decryption time costs of RSA, CP-ABE, ABSE, and the proposed algorithm were 10.2 ms, 6.5 ms, 5.2 ms, and 5.8 ms, respectively. When the amount of attributes reached 35, the decryption time costs of the four algorithms were 73.9 ms, 39.7 ms, 32.5 ms, and 33.0 ms, respectively. The findings denote that the designed method can achieve good encryption and decryption efficiency while ensuring privacy.

Further comparative analysis was conducted on the encryption and decryption time overhead of different EAs under different data file sizes, and the findings are denoted in Figure 9. In Figure 9(a), when the data file size was 2MB, the encryption time costs of RSA, CP-ABE, and ABSE were 15.2 ms, 10.5 ms, and 9.1 ms, respectively, and the encryption time cost of the proposed algorithm was 8.3ms. When the data file size was 64 MB, the encryption time costs of the four algorithms were 428.9 ms, 295.6 ms, 251.7 ms, and 234.1 ms, respectively. In Figure 9(b), when the file data

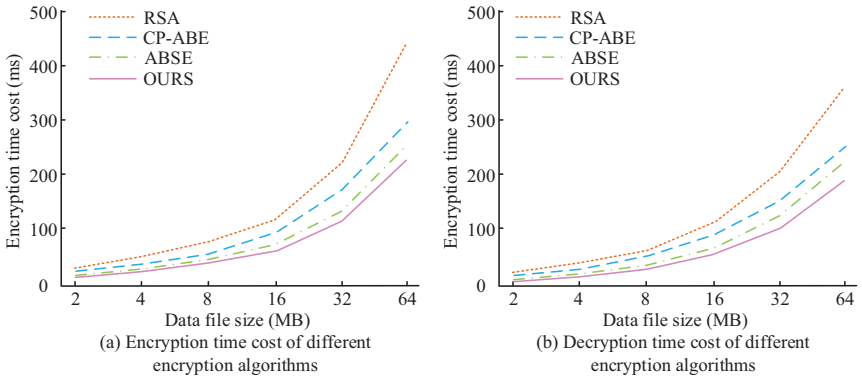


Figure 9 The encryption and decryption time cost of different EAs under different data file sizes.

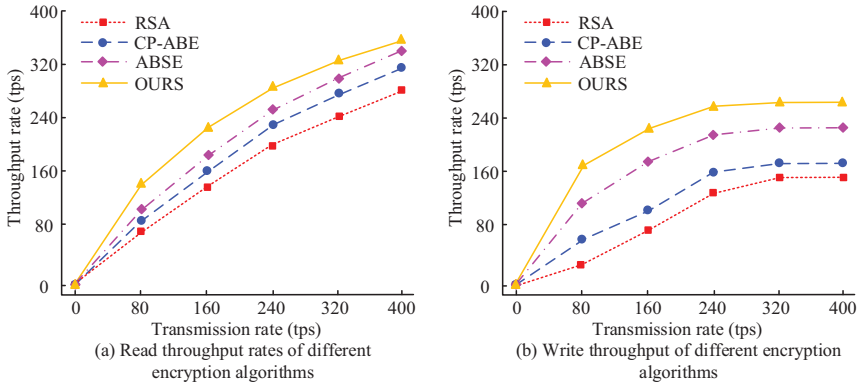


Figure 10 Read throughput and write throughput of different EAs at different transmission rates.

size was 2 MB, the decryption time costs of RSA, CP-ABE, ABSE, and the proposed algorithm were 12.8 ms, 8.7 ms, 7.6 ms, and 6.9 ms, respectively. When the file data size reached 64 MB, the encryption time costs of the four algorithms were 365.1 ms, 251.8 ms, 218.6 ms, and 199.1 ms. The outcomes demonstrate that the designed algorithm performs better than the compared algorithms in terms of encryption and decryption efficiency, demonstrating better overall performance.

A comparative analysis of the read and write throughput of different EAs at various transmission rates was conducted to evaluate the system's data processing capability in high concurrency scenarios. The findings are denoted in Figure 10. In Figure 10(a), when the transmission rate was 80 tps, the read

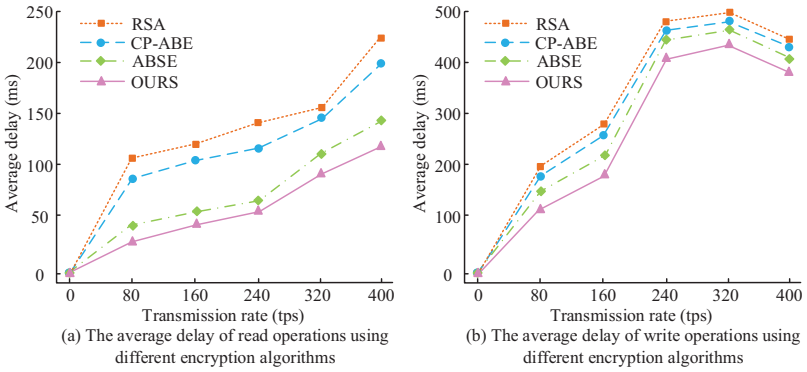


Figure 11 The average delay of read and write operations for different EAs.

throughput rates of RSA, CP-ABE, ABSE, and the proposed algorithm were 72 tps, 80 tps, 96 tps, and 137 tps, respectively. When the sending rate reached 400 tps, the read throughput rates of the four algorithms were 280 tps, 315 tps, 332 tps, and 342 tps, respectively. In Figure 10(b), when the transmission rate was 80 tps, the write throughput rates of RSA, CP-ABE, ABSE, and the proposed algorithm were 39 tps, 58 tps, 113 tps, and 168 tps. When the sending rate increased to 400 tps, the write throughput rates of the four algorithms were 142 tps, 168 tps, 219 tps, and 252 tps, respectively. It was found that the proposed algorithm maintains good throughput performance under high transmission loads and is suitable for high-frequency data access scenarios in LSCs.

The average delay of read and write operations for different EAs was compared at different transmission rates, and the findings are denoted in Figure 11. In Figure 11(a), when the transmission rate was 80 tps, the average read operation delays of RSA, CP-ABE, and ABSE were 108.2 ms, 81.5 ms, and 39.6 ms, respectively, and the average delay of the proposed algorithm was 26.7 ms. When the transmission rate reached 400 tps, the average read operation delays of the four algorithms were 224.3 ms, 202.8 ms, 129.5 ms, and 109.4 ms. In Figure 11(b), when the transmission rate was 80 tps, the average write operation delays of RSA, CP-ABE, ABSE, and the proposed algorithm were 198.6 ms, 180.3ms, 142.7ms, and 108.9ms, respectively. At a throughput of 320 TPS, the four algorithms exhibited their maximum average write latency, measuring 498.2 ms, 481.6 ms, 459.7 ms, and 428.9 ms respectively. The findings denote that the designed algorithm performs better than other compared algorithms in terms of average delay performance for read and write operations, demonstrating the reliability of the algorithm.

3.2 Performance Analysis and Testing of LSCMS

To assess the effect of the designed LSCMS, a simulation of multi-party participation scenarios in a real LSC was studied and compared with current mainstream management systems. These included Single Blockchain Logistics System (SBLS), Consortium Blockchain-based Logistics Tracking System (CBLTS), and Hybrid Cloud-Blockchain Logistics Platform (HCBLP).

The throughput, transaction confirmation delay, Central Processing Unit (CPU) utilization, and memory usage of different comparison systems were tested under low and high loads, and the findings are denoted in Figure 12. In Figure 12(a), the throughput of SBLS, CBLTS, and HCBLP under low load was 121 tps, 186 tps, and 218 tps, respectively, while under high load it was 282 tps, 341 tps, and 395 tps, respectively. The throughput of the proposed system under low load and high load was 252 tps and 449 tps,

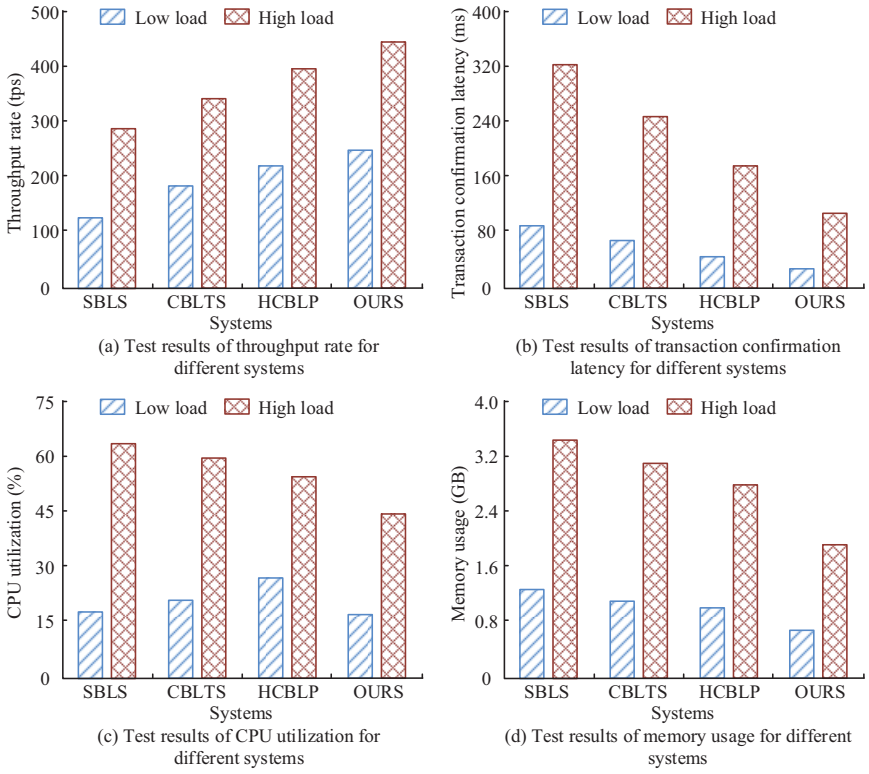


Figure 12 Performance test results of different comparison systems.

respectively. In Figure 12(b), the transaction confirmation delays of SBLS, CBLTS, HCBLP, and the proposed system under low load were 86.2 ms, 64.3 ms, 45.5 ms, and 31.2 ms, respectively. The transaction confirmation delays under high load were 321.8 ms, 242.6 ms, 185.3 ms, and 116.9 ms, respectively. In Figure 12(c), the CPU utilization rates of the four systems under low load were 18.1%, 18.1%, 18.1%, and 18.1%, respectively, and under high load were 18.1%, 18.1%, 18.1%, and 18.1%, respectively. In Figure 12(d), the memory usage of the four systems under low load was 1.2 GB, 1.0 GB, 0.9 GB, and 0.7 GB, respectively, while under high load it was 3.5 GB, 3.1 GB, 2.8 GB, and 2.2 GB, respectively. The findings denote that the designed system performs better than existing solutions in terms of throughput performance, transaction confirmation efficiency, resource utilization efficiency, and memory management, and has better scalability and real-time processing capabilities.

The performance of the cross-chain communication mechanism under increasing transaction loads was evaluated, with results summarized in Table 3. It was observed that the bandwidth consumption increased linearly with the transaction load, which is attributed to the growing volume of Merkle root hashes and transaction metadata requiring relay between the main chain and the regulatory blockchain. The consensus time, primarily governed by the node rotation mechanism on the regulatory chain, also experienced a moderate increase due to the heightened communication overhead for node coordination and state verification under higher loads. Crucially, even at a load of 200 cross-chain transactions per second, the success rate remained high at 97.2%, demonstrating the robustness of the proposed dual-chain architecture and its associated communication protocol.

The study analyzed the communication overhead and consensus time of different systems under different plaintext lengths, and the findings are

Table 3 Performance metrics for cross-chain communication under varying transaction loads

Cross-chain Transaction Load (TPS)	Average Bandwidth Consumption (Kbps)	Peak Bandwidth Consumption (Kbps)	Consensus Time (ms)	Cross-chain Success Rate (%)
500	128.5	185.2	105.4	99.1
100	245.8	351.7	118.9	98.5
150	268.3	528.1	136.2	97.9
200	489.6	702.4	155.7	97.6
250	612.0	878.5	178.3	97.2

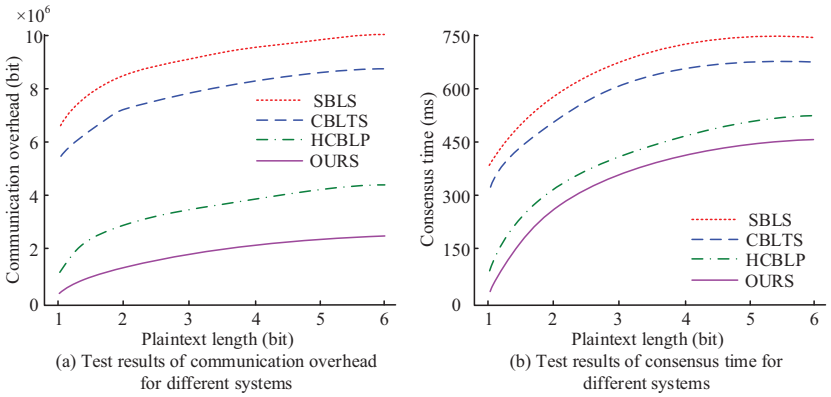


Figure 13 Comparison of communication overhead and consensus time among different systems.

denoted in Figure 13. In Figure 13(a), when the plaintext length was 1 bit, the communication overhead of SBLS, CBLTS, HCBLP, and the proposed system were 6.4×10^6 bit, 5.5×10^6 bit, 1.1×10^6 bit, and 0.4×10^6 bit, respectively. When the plaintext length reached 6 bits, the communication overhead of the four systems is 9.2×10^6 bit, 8.1×10^6 bit, 4.0×10^6 bit, and 1.8×10^6 bit. In Figure 13(b), when the plaintext length was 1 bit, the consensus times of SBLS, CBLTS, HCBLP, and the proposed system were 426.3 ms, 329.8 ms, 86.7 ms, and 31.5 ms, respectively. When the plaintext length was increased to 6 bits, the consensus times of the four systems were 739.6 ms, 658.9 ms, 496.7 ms, and 402.3 ms, respectively. The findings denote that the designed system can minimize network load and processing delay during operation, and has higher communication and consensus efficiency.

The study tested the data storage efficiency and security audit efficiency of different systems, and the findings are denoted in Table 4. In Table 4, in terms of data storage efficiency, the original data volume of the proposed system was 10.8 GB, which is 6.5 GB after compression. The compression ratio reached 39.8%, which means that the original data is compressed to about 60% of its size, 3–7 percentage points higher than the comparison system, significantly reducing on chain storage costs. In terms of security audit efficiency, the average processing time of the proposed system was 5.4 ms, the max processing time was 15.1 ms, and the audit accuracy was as high as 98.7%. In addition, the p-values of compression ratio and audit accuracy were both less than 0.05. The findings denote that the designed

Table 4 Test results of data storage efficiency and security audit efficiency

Test Projects	Indicators	SBLS	CBLTS	HCBLP	OURS	p-value
Data	Raw data volume (GB)	13.2	12.5	11.5	10.8	/
storage	Compressed data volume (GB)	8.9	8.2	7.3	6.5	/
efficiency	Compression ratio (%)	32.6	34.4	36.5	39.8	<0.05
Security	Average processing time (ms)	18.5	12.2	8.8	5.4	/
audit	Maximum processing time (ms)	45.2	32.8	25.5	15.1	/
efficiency	Audit accuracy rate (%)	88.5	92.0	95.3	98.7	<0.05

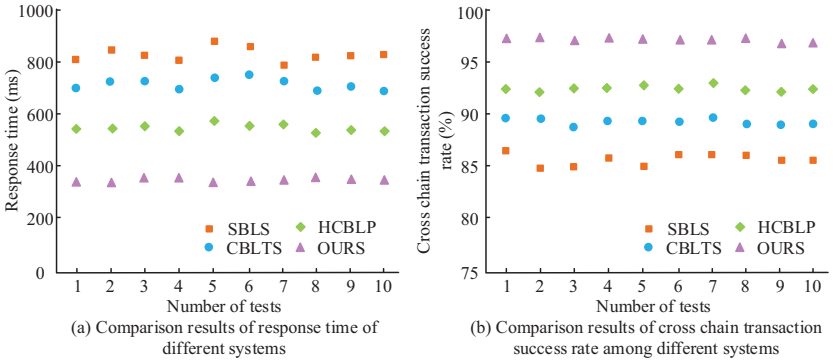
Table 5 Comparison of system performance under different numbers of network nodes

System Architecture	Performance Metric	4 Nodes	8 Nodes	16 Nodes	32 Nodes
SBLS	Throughput (TPS)	282	245	498	152
	Latency (ms)	321.8	358.4	425.1	532.6
CBLTS	Throughput (TPS)	341	312	268	215
	Latency (ms)	242.6	275.3	328.7	412.9
HCBLP	Throughput (TPS)	395	372	335	286
	Latency (ms)	185.3	209.8	254.3	325.6
OURS	Throughput (TPS)	449	421	385	332
	Latency (ms)	116.9	138.5	172.1	231.7

system can achieve faster and more accurate security auditing while ensuring streamlined data storage.

To further explore the horizontal scalability of the proposed system, the throughput and transaction confirmation delay of different comparison systems were analyzed under different numbers of network nodes. The results are shown in Table 5. In Table 5, as the number of nodes increased from 4 to 32, the performance of each system decreased. The proposed system has a throughput of 449 TPS and a latency of 116.9 ms at 4 nodes, both of which are superior to the compared systems. At 32 nodes, the proposed system throughput is 332 TPS, still higher than SBLS, CBLTS, and HCBLP, with a latency of 231.7 ms. The results show that the proposed system has significant advantages in scalability, with smoother performance degradation and better adaptability to large-scale node environments.

To verify the superiority of the designed system, the response time and cross chain transaction success rate of different systems were analyzed, and the findings are denoted in Figure 14. In Figure 14(a), the average response times of SBLS, CBLTS, and HCBLP were 812.7 ms, 696.8 ms, and 548.2 ms, respectively. Compared with them, the average response time of the proposed system was 342.5 ms, which was shortened by 57.9%, 50.8%, and 37.5%,



(a) Comparison results of response time of different systems

(b) Comparison results of cross chain transaction success rate among different systems

Figure 14 Response time and cross chain transaction success rate of different systems.

respectively. In Figure 14(b), the average cross chain transaction success rates of SBLS, CBLTS, HCBLP, and the proposed system were 85.2%, 89.4%, 92.3%, and 97.6%. Compared with the comparison system, the cross chain transaction success rate of the proposed system increased by 12.4%, 8.2%, and 5.3%. The findings indicate that the designed system can effectively minimize transaction processing latency and strengthen the reliability and success rate of cross chain transactions.

The study conducted a quantitative analysis of the computational and storage overhead of the proposed system and the comparative system, as shown in Table 6. In Table 6, the system mentioned had the highest average CPU core occupancy per node under high load, at 5.5 cores, with the highest storage I/O requirements at 58.7 MB/s, and the highest network bandwidth requirements at 105 Mbps, indicating significant computational and communication overhead. But its memory usage was the lowest, at 2.2 GB, and only required 4 GB of memory in the minimum hardware configuration, which is better than other comparative systems that require 8 GB, reflecting its high efficiency in memory usage. Overall, the proposed system has achieved significant memory efficiency advantages in exchange for higher computing and communication costs.

4 Conclusion

A privacy protection method for LSC based on blockchain and ABE algorithm was designed, and a multi-blockchain collaborative LSCMS was constructed. The findings denoted that the proposed privacy protection method performed excellently in terms of encryption and decryption efficiency. When

Table 6 Quantitative analysis of computing and storage costs in different systems

Indicators	SBLS	CBLTS	HCBLP	OURS
Average CPU Cores Utilized per Node (Under High Load)	4.2	4.5	4.8	5.5
Average RAM Utilization per Node (Under High Load)	3.5	3.1	2.8	2.2
Average Storage I/O per Node (Under High Load, MB/s)	45.8	48.1	52.3	58.7
Estimated Minimum Network Bandwidth per Node (Mbps)	85	90	95	105
Estimated Minimum Node Hardware Recommendation	8-core CPU, 8 GB RAM, 500 GB SSD	8-core CPU, 8 GB RAM, 500 GB SSD	8-core CPU, 8 GB RAM, 500 GB SSD	8-core CPU, 4 GB RAM, 500 GB SSD

the amount of attributes was 35, the encryption and decryption time overhead were 41.5 ms and 33.0 ms, respectively. When the data file size was 64 MB, the encryption and decryption time were 234.1 ms and 199.1 ms, respectively, which was better than mainstream algorithms such as RSA, CP-ABE, and ABSE. Meanwhile, in high concurrency scenarios, the proposed method achieved a read throughput of 342 tps and a write throughput of 252 tps, with average read and write delays of 109.4 ms and 428.9 ms, respectively, demonstrating good real-time performance and reliability. In terms of system performance, the proposed management system had throughput of 252 tps and 449 tps under low and high loads, respectively, and transaction confirmation delays of 31.2 ms and 116.9 ms, all of which were superior to comparative systems such as SBLS, CBLTS, and HCBLP. The findings indicate that the designed system has comprehensive capabilities of high efficiency, security, and trustworthiness in LSC management. However, to successfully transition this research from laboratory environments to practical industrial applications, several critical challenges must be prioritized. First, the system's operational overhead and associated costs in a real-world, multi-party consortium setting need to be rigorously evaluated and optimized. This includes the computational costs of continuous ABE operations and the infrastructure costs of maintaining multiple blockchain nodes. Second, seamless integration with legacy enterprise systems and diverse logistics platforms must be addressed through the development of robust, standardized APIs and

adaptable data models. Finally, establishing a sustainable and incentivized governance model for the consortium blockchain is paramount, defining clear rules for node membership, transaction fees, and dispute resolution to ensure long-term viability and adoption.

Furthermore, the feasibility of integrating the proposed system with existing logistics platforms – such as SF Express and JD Logistics – has been preliminarily analyzed. The hierarchical blockchain architecture and standardized smart contract interfaces are designed to be compatible with common data exchange protocols and legacy enterprise systems. For instance, in scenarios like cold-chain pharmaceutical traceability or cross-border parcel tracking, the system can be deployed as a modular privacy-enhancing layer, interfacing with existing logistics execution systems via API gateways. This allows for incremental adoption without disrupting core operations, while providing enhanced data security, FGAC, and regulatory compliance capabilities.

The limitation of this study is that it did not consider long-term operational validation in real large-scale logistics networks. SWOT analysis further reveals the actual constraints of the system: the advantage lies in FGAC and efficient cross chain collaboration. The disadvantage lies in the significant increase in ABE computational overhead and non-linear increase in management complexity when the attribute scale expands. The opportunity lies in connecting with platforms such as SF Express and JD.com to empower cross-border traceability scenarios. The main threats come from the ongoing operational costs of multi node blockchain and the bandwidth bottleneck of high concurrency cross chain communication. These quantitative constraints need to be continuously optimized in actual deployment. Therefore, future research will mainly focus on the following three aspects: deploying verification systems in real-world logistics alliance chains to quantitatively assess cross-chain communication bandwidth and attribute management costs; exploring lightweight EAs and sharding technologies to reduce computational overhead; and researching dynamic authorization optimization models to improve permission management efficiency in complex SC scenarios.

Acknowledgement

This study is funded by the following projects: Zhenjiang Soft Science Project (No. RK2024032); Jiangsu Provincial Federation of Social Sciences Excellent Project (No. 73); Philosophy and Social Sciences Research Project for Universities in Jiangsu Province (No. 2023SJYB2240).

Appendix

Table A1 The original test dataset for compression ratio and audit accuracy rate

Run No.	Raw Data Volume (GB)	Compressed Data Volume (GB)	Compression Ratio (%)	Audit Accuracy Rate (%)
1	10.8	6.5	39.8	98.7
2	10.9	6.6	39.4	98.5
3	10.8	6.5	39.8	98.8
4	10.7	6.4	40.2	98.9
5	10.8	6.5	39.8	98.6
6	10.9	6.6	39.4	98.7
7	10.8	6.5	39.8	98.8
8	10.7	6.4	40.2	98.9
9	10.8	6.5	39.8	98.7
10	10.9	6.6	39.4	98.6

References

[1] Wei M. Optimization of Emergency Material Logistics Supply Chain Path Based on Improved Ant Colony Algorithm. Informatica, 2025, 49(16): 187–198. DOI: 10.31449/inf.v49i16.7452.

[2] Kazancoglu Y, Ozbiltekin-Pala M, Sezer MD, Luthra S, and Kumar A. Resilient reverse logistics with blockchain technology in sustainable food supply chain management during COVID-19. Business Strategy and the Environment, 2023, 32(4): 2327–2340. DOI: 10.1002/bse.3251.

[3] Ogbuke NJ, Yusuf YY, Dharma K, and Mercangoz BA. Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 2022, 33(2–3): 123–137. DOI: 10.1080/09537287.2020.1810764.

[4] Li L, Gong Y, Wang Z, and Liu S. Big data and big disaster: a mechanism of supply chain risk management in global logistics industry. International Journal of Operations & Production Management, 2023, 43(2): 274–307. DOI: 10.1108/IJOPM-04-2022-0266.

[5] Xu X and He Y. Blockchain application in modern logistics information sharing: A review and case study analysis. Production Planning & Control, 2024, 35(9): 886–900. DOI: 10.1080/09537287.2022.2058997.

[6] Van Nguyen T, Cong Pham H, Nhat Nguyen M, Zhou L, and Akbari M. Data-driven review of blockchain applications in supply chain management: key research themes and future directions. International

Journal of Production Research, 2023, 61(23): 8213–8235. DOI: 10.1080/00207543.2023.2165190.

[7] Wei Q, Li B, Chang W, Jia Z, Shen Z, and Shao Z. A survey of blockchain data management systems. ACM Transactions on Embedded Computing Systems (TECS), 2022, 21(3): 1–28. DOI: 10.1145/3502741.

[8] Gudala L, Reddy AK, Sadhu AKR, and Venkataramanan S. Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. Journal of Artificial Intelligence Research, 2022, 2(2): 21–50. DOI: 10.1007/978-981-97-8355-7_44.

[9] Das D, Banerjee S, Chatterjee P, Biswas M, Biswas U, and Alnumay W. Design and development of an intelligent transportation management system using blockchain and smart contracts. Cluster computing, 2022, 25(3): 1899–1913. DOI: 10.1007/s10586-022-03536-z.

[10] Yang C, Lan S, Zhao Z, Zhang M, Wu W, and Huang GQ. Edge-cloud blockchain and IoE-enabled quality management platform for perishable supply chain logistics. IEEE Internet of Things Journal, 2022, 10(4): 3264–3275. DOI: 10.1109/JIOT.2022.3142095.

[11] Vidhya S and Kalaivani V. A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. Peer-to-Peer Networking and Applications, 2023, 16(2): 900–913. DOI: 10.1007/s12083-023-01449-1.

[12] Ping J, Yan Z, and Chen S. A privacy-preserving blockchain-based method to optimize energy trading. IEEE Transactions on Smart Grid, 2022, 14(2): 1148–1157. DOI: 10.1109/TSG.2022.3198165.

[13] Jiang Y, Xu X, and Xiao F. Attribute-based encryption with blockchain protection scheme for electronic health records. IEEE Transactions on Network and Service Management, 2022, 19(4): 3884–3895. DOI: 10.1109/TNSM.2022.3193707.

[14] Wan J, Hu K, Li J, and Su H. AnonymousFox: An efficient and scalable blockchain consensus algorithm. IEEE Internet of Things Journal, 2022, 9(23): 24236–24252. DOI: 10.1109/JIOT.2022.3189200.

[15] Zhang K, Zhang Y, Li Y, Liu X, and Lu L. A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing. IEEE Internet of Things Journal, 2023, 11(1): 1685–1697. DOI: 10.1109/JIOT.2023.3290975.

[16] Datta S and Namasudra S. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and

mobile-edge computing. IEEE Transactions on Consumer Electronics, 2024, 70(1): 4026–4036. DOI: 10.1109/TCE.2024.3357115.

[17] Richey Jr RG, Chowdhury S, Davis-Sramek B, Giannakis M, and Dwivedi YK. Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. Journal of Business Logistics, 2023, 44(4): 532–549. DOI: 10.1111/jbl.12364.

[18] Jalali NA and Hongsong C. Comprehensive framework for implementing blockchain-enabled federated learning and full homomorphic encryption for chatbot security system. Cluster Computing, 2024, 27(8): 10859–10882. DOI: 10.1007/s10586-024-04515-2.

[19] Rasori M, La Manna M, Perazzo P, and Dini G. A survey on attribute-based encryption schemes suitable for the internet of things. IEEE Internet of Things Journal, 2022, 9(11): 8269–8290. DOI: 10.1109/JIOT.2022.3145726.

[20] Yang Y, Zhang J, Liu X, and Ma J. A scalable and auditable secure data sharing scheme with traceability for fog-based smart logistics. IEEE Internet of Things Journal, 2022, 10(10): 8603–8617. DOI: 10.1109/JIOT.2022.3220850.

[21] Richey RG, Roath AS, Adams FG, and Wieland A. A responsiveness view of logistics and supply chain management. Journal of Business Logistics, 2022, 43(1): 62–91. DOI: 10.1111/jbl.12290.

[22] Chen Z, Liu F, Li D, Liu Y, Yang X, and Zh, H. Video security in logistics monitoring systems: a blockchain based secure storage and access control scheme. Cluster Computing, 2024, 27(8): 10245–10264. DOI: 10.1007/s10586-024-04667-1.

[23] Yi X, Zhou Y, Lin Y, Xie B, Chen J, and Wang C. Digital rights management scheme based on redactable blockchain and perceptual hash. Peer-to-peer Networking and Applications, 2023, 16(5): 2630–2648. DOI: 10.1007/s12083-023-01552-3.

[24] Escobar CC, Roy S, Kreidl OP, Dutta A, and Bölöni L. Toward a green blockchain: Engineering merkle tree and proof of work for energy optimization. IEEE Transactions on Network and Service Management, 2022, 19(4): 3847–3857. DOI: 10.1109/TNSM.2022.3219494.

[25] Yang F, Qiao Y, Qi Y, Bo J, and Wang X. BACS: blockchain and AutoML-based technology for efficient credit scoring classification. Annals of Operations Research, 2025, 345(2): l703–723. DOI: 10.1007/s10479-022-04531-8.

Biographies

Ying Chen, female, born in June 1987, graduated from Southwest Jiaotong University with a master's degree in logistics engineering. After graduation, she worked as a manager in a large logistics enterprise and is currently employed as a lecturer at Jiangsu Aviation Vocational and Technical College. Her research interests include supply chain management and aviation logistics service chain management.

Xiaojuan Yue, female, born in October 1987, graduated from Southwest Jiaotong University with a master's degree in logistics engineering. After graduation, she worked as a lecturer at Chongqing University of Finance and Economics, with a research focus on green logistics and supply chain management.

Wang Pan, male, August 1995, graduated from Cardiff University in the UK with a master's degree in logistics and operations management. He is currently employed as a lecturer at Jiangsu Aviation Vocational and Technical College, with a research focus on supply chain management and aviation logistics service chain management.