scientific reports

Check for updates

OPEN

A cross-chain model for warehouse receipts in port supply chain based on notary mechanism and ShangMi cryptographic algorithms

Yangbo Chen[1], Wei Ou[1,2,3]✉, Mengxue Pang[1], Jianqiang Ma[1], Qiuling Yue[1] & Wenbao Han[1]

In the evolving landscape of global trade digitalization, port supply chains play a pivotal role as critical components of international logistics. These supply chains face pressing needs to enhance the efficiency and security of warehouse receipt management. Traditional methods often grapple with challenges such as information isolation, vulnerabilities in data security, and suboptimal collaboration efficiency. This paper introduces a novel cross-chain warehouse receipt management system that leverages a notary mechanism and ShangMi (SM) cryptographic algorithms to overcome these obstacles. The system is structured around an innovative "3 + 1" multi-chain architecture, which consists of three distinct business chains—production, port, and sales—and a cross-chain management platform that orchestrates communication between these chains. The proposed system employs a layered data structure for warehouse receipts and uses differentiated encryption strategies. These features enable flexible data sharing while ensuring the protection of sensitive information. To further enhance operational efficiency, the system incorporates performance optimization strategies such as batch processing and incremental synchronization. Experimental evaluations reveal significant performance improvements over conventional systems. For instance, under conditions of 800 concurrent users, our system achieves a query latency of 485.3 milliseconds (ms) compared to 7,900 ms in the reference system, and maintains a query throughput of 565.4 transactions per second (TPS), in stark contrast to approximately 100TPS in the reference system. These results underscore the technical superiority of our approach in practical business scenarios.

Keywords Port supply chain, Warehouse receipt management, Cross-chain technology, Notary mechanism, ShangMi cryptographic algorithms

The rapid digitalization of global commerce has positioned port supply chains as essential facilitators in enhancing the efficiency of cross-border trade and bolstering global competitiveness[1,2]. Within these supply chains, warehouse receipts are pivotal documents that affirm ownership and governance of goods, with their management efficacy critically influencing the overall operational quality of the supply chain[3,4]. Conventional management of warehouse receipts encounters numerous challenges: paper-based receipts are prone to damage and issues related to authenticity verification, limited information sharing across various stakeholders leads to operational inefficiencies, and concerns over data security and privacy protection are increasingly acute[5]. These issues have stimulated considerable research in both the academic and industrial realms.

Initial studies predominantly concentrated on enhancing traditional supply chain management systems. Li et al.[6] developed an optimization framework for warehouse receipt management through business process reengineering, standardization of document formats, and integration of information systems. Their methodology facilitated initial stages of data sharing and business collaboration, yet challenges related to data privacy protection and system security remained unresolved. Cândido et al.[7] examined a Service-Oriented Architecture (SOA)-based approach for integrating supply chain information, which proved to improve system flexibility and interoperability. In a similar vein, Giannakis et al.[8] assessed the potential of cloud computing in supply chain management and introduced a collaborative framework that utilizes cloud platforms. Additionally, Selvakumar and Jayashree[9] promoted enhanced supply chain collaboration through the adoption of a microservices

[1]School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China. [2]Laboratory for Advanced Computing and Intelligence Engineering, Wuxi 214100, China. [3]Jiangsu Variable Supercomputer Technology Co., Ltd, Wuxi 214100, China. ✉email: ouwei@hainanu.edu.cn

architecture, which notably augmented system scalability and maintainability. Despite these technological advances, significant obstacles still exist in ensuring data security and system reliability, particularly in scenarios that require secure data sharing and precise access control mechanisms in multi-party collaborations. Moreover, cross-organizational data exchanges continue to face systemic challenges, including vulnerabilities in data transmission protocols and inefficiencies in coordinating operations in real-time.

The advent of blockchain technology has heralded a transformative era in the management of warehouse receipts. Lee and Yeon[10] conducted a systematic examination of blockchain's application architectures within supply chains, with a particular emphasis on the deployment of smart contracts for automating business processes and facilitating multi-party collaboration. This work offers fresh insights into the digital transformation of supply chains. Liu et al.[11] presented innovative solutions for controllable blockchain data management, featuring uniquely designed differentiated data access control mechanisms. Furthermore, Xue and Wang[12] investigated privacy protection schemes utilizing zero-knowledge proofs, which ensure verifiable information sharing while safeguarding sensitive data. To enhance the security and efficiency of cross-chain transactions, Hu et al.[13] proposed a blockchain-based cross-chain transaction method incorporating decentralized dynamic reputation value evaluation. While this approach strengthens transaction reliability through real-time credibility assessment of participants, it primarily focuses on transaction-layer security while inadequately addressing data stratification requirements and fine-grained access control mechanisms inherent in supply chain scenarios. More critically, the optimization strategies demonstrate excessive specificity toward particular application contexts. For instance, Amico et al.[14] conducted quantitative analyses and case studies to evaluate blockchain-empowered bills of lading in port supply chain enhancement, revealing the technology's potential in fraud mitigation and operational transparency improvement. However, their research predominantly emphasizes document digitization rather than comprehensively resolving the multidimensional complexities in warehouse receipt management. Similarly, Xie et al.[15] designed a blockchain-based financial platform for port logistics, aiming to optimize financing efficiency and risk control. Nevertheless, its architecture overly prioritizes financial service integration while insufficiently addressing multi-party data interoperability and cross-chain operation demands essential for warehouse receipt management.

In summary, existing blockchain or cross-chain system-based solutions still face limitations in data stratification, cross-chain interoperability, and optimization of specific business processes: (1) Existing cross-chain systems lack fine-grained encryption strategies for managing data with varying sensitivity levels, making it challenging to achieve flexible sharing while ensuring data security[16,17]. (2) In high-concurrency scenarios, particularly in complex warehouse receipt management systems involving multi-party collaboration, the efficiency of cross-chain business processes still fails to adequately meet practical business demands[18]. (3) Existing systems primarily rely on single-chain structures or oversimplified cross-chain mechanisms, rendering them incapable of effectively supporting the complex business scenarios of multi-party collaboration in port supply chains[19].

Based on the limitations of current research, this paper aims to achieve the following research objectives: First, to construct a cross-chain architecture capable of supporting multi-party collaboration in port supply chains, ensuring data isolation while enabling secure and controlled data sharing; second, to develop encryption strategies suitable for data with different sensitivity levels, balancing the requirements of data security and sharing efficiency; finally, to enhance system response speed and throughput for high-concurrency scenarios, meeting practical business requirements.

To address these research objectives, this paper proposes a cross-chain warehouse receipt management system based on a notary mechanism and ShangMi cryptographic algorithms. The system employs an innovative "3 + 1" multi-chain architecture, comprising three business chains (production chain, port chain, and sales chain) and a cross-chain management platform, achieving physical isolation while ensuring secure data sharing. Through layered data structures and differentiated encryption strategies, the system employs various ShangMi algorithms to protect data of different sensitivity levels, ensuring both flexibility and security in data sharing. Furthermore, the system incorporates optimization strategies such as batch processing, incremental synchronization, and parallel processing, significantly enhancing system performance in high-concurrency environments. The primary contributions of this research are as follows:

- Propose a cross-chain collaboration model based on a "3 + 1" multi-chain architecture. This model effectively coordinates business chains and unifies cross-chain communication management, addressing data silo challenges while ensuring secure data sharing.
- Implement a differentiated encryption and smart contract system using layered data structures and SM cryptographic algorithms. This system provides robust protection and flexible access to sensitive data while automating key business processes to enhance collaboration.
- Demonstrate significant performance improvements through extensive testing in high-concurrency environments. The system maintains a stable query throughput near 720TPS under 1000–1400 concurrent users, achieves an average query latency below 600ms, and sustains a transaction throughput of approximately 250TPS.

The remainder of this paper is structured as follows: section "Preliminaries" introduces preliminary concepts including SM cryptographic algorithms and the notary mechanism; section "System design" details the system design, including the overall architecture and main functions; section "Experiments and analysis" presents a comprehensive performance evaluation and comparative analysis; section "Research findings and managerial implications" presents research findings and managerial implications; and section "Conclusion and future work" concludes the paper and outlines directions for future research.

Preliminaries

Block

Blockchain technology, first proposed by Nakamoto[20] in 2008, operates as a decentralized distributed ledger that chronologically links records (termed blocks) through cryptographic hashing. Each block encapsulates transaction data, and once appended to the chain, becomes immutable without network consensus, thereby ensuring data integrity. The technology's principal advantage lies in its decentralized nature, where multiple nodes collectively maintain ledger replicas without requiring central authority, significantly enhancing security and transparency[10,21,22]. Smart contracts—a critical blockchain component—function as self-executing agreements with terms directly encoded, automatically enforcing contractual obligations upon predefined condition fulfillment, thereby streamlining processes and mitigating operational risks[23].

Blockchain has broad application prospects in the fields of supply chain management and warehouse receipt management[4,24]. In the supply chain, blockchain enables transparency, verifiability and secure tracking of goods and services, ensuring data integrity and operational efficiency[11,15]. For warehouse receipt management, the technology can create verifiable digital warehouse receipts and safely transfer them between parties in the supply chain, reducing the risk of traditional paper warehouse receipts[3,25]. Furthermore, blockchain supports secure data exchange across disparate networks while ensuring authenticated information flow[26]. This technology is gradually changing the operating model of all industries by providing safe, transparent and efficient solutions.

Notary mechanism

The notary mechanism, as depicted in Fig. 1, serves as a cross-chain operational framework that facilitates secure interactions among diverse blockchain networks. It fundamentally employs a distributed network of trusted nodes that function as intermediaries, thereby enabling and validating cross-chain operations. These notary nodes utilize specialized consensus protocols to authenticate requests and ensure data consistency across different chains[27]. The mechanism executes a two-phase validation process: initially, notary nodes independently assess the validity of cross-chain requests based on predefined criteria; subsequently, they collaboratively achieve consensus on the verification outcomes through a distributed voting mechanism. Distinct from traditional blockchain interoperability solutions, which depend on elaborate cryptographic proofs or token-based bridges, the notary mechanism adopts a trust-based validation model. This model offers enhanced flexibility and efficiency by significantly reducing computational demands, while still providing robust security assurances through its distributed trust architecture.

SM cryptographic algorithms

The SM cryptographic algorithms, developed under the auspices of the State Cryptography Administration of China, represent a comprehensive array of national cryptographic standards that include symmetric encryption, asymmetric encryption, and hashing algorithms. This suite specifically comprises the SM1, SM4, SM7, and

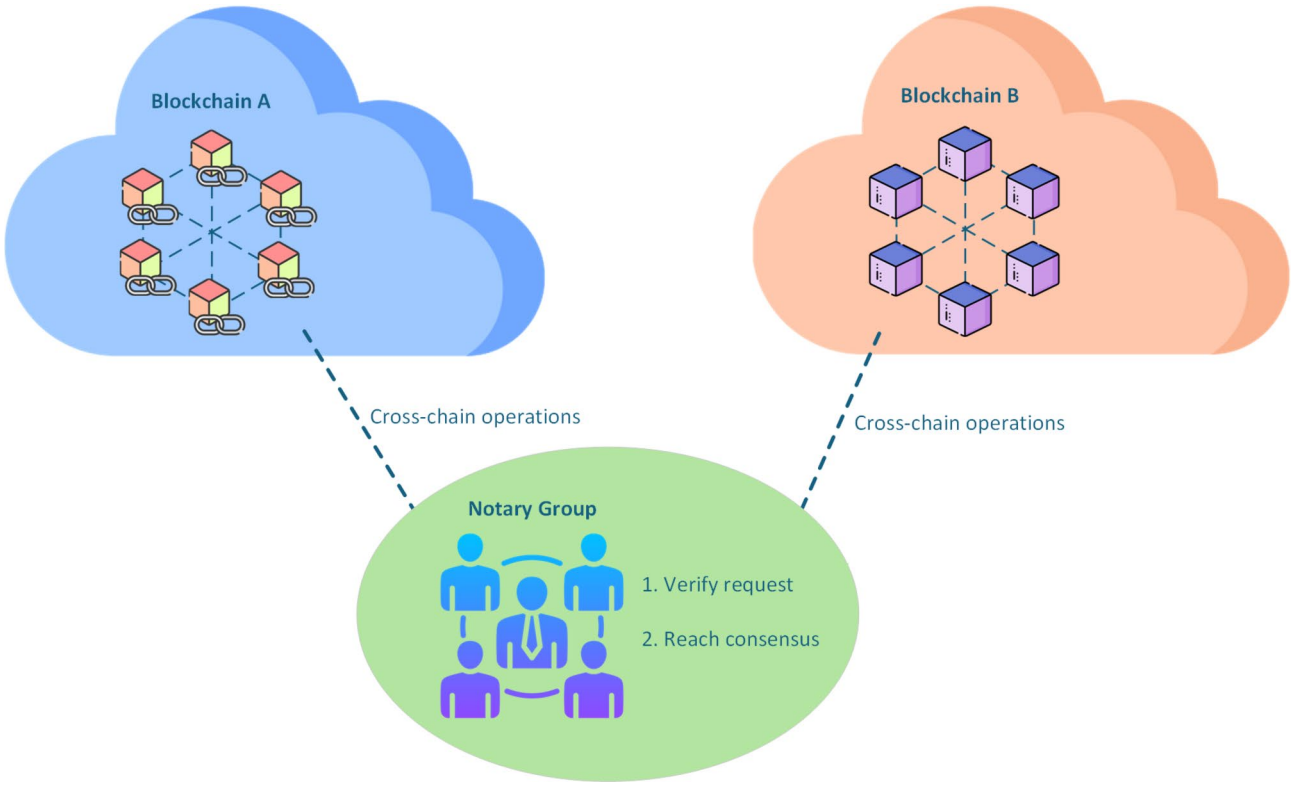

Fig. 1. Notary mechanism.

ZUC algorithms for symmetric encryption; SM2 and SM9 for asymmetric encryption; and SM3 for hashing operations[28]. This section will detail the SM2, SM3, and SM4 algorithms as utilized in our proposed system.

SM2: The SM2 algorithm, which is the primary public-key cryptographic system in the SM series, operates on a 256-bit prime field. It utilizes carefully chosen curve parameters based on Elliptic Curve Cryptography (ECC). The algorithm is designed to perform three primary functions: digital signatures, key exchange, and public-key encryption. Its security foundation is the Elliptic Curve Discrete Logarithm Problem (ECDLP), which provides a level of computational security comparable to a 3072-bit RSA key, albeit with much shorter key lengths. The design of SM2 includes several distinctive features, such as the integration of message digest computation and additional verification mechanisms, which enhance its resistance to a variety of cryptographic attacks.

SM3: The SM3 cryptographic hash function features a design akin to SHA-256 but includes unique elements in its compression function. Operating on 512-bit message blocks, SM3 generates 256-bit hash values and employs an advanced Merkle-Damgård construction with additional security enhancements. The compression function executes 64 rounds of operations that involve optimized message expansion and specially designed constant parameters. These operations facilitate robust collision resistance and preimage resistance, rendering SM3 appropriate for applications in digital signature generation, message authentication, and random number generation.

SM4: The SM4 algorithm is a symmetric block cipher that utilizes a 128-bit block structure and a key length of 128 bits. It is structured around a 32-round Substitution-Permutation Network (SPN) architecture. The encryption and decryption processes in SM4 are unified, where each round includes nonlinear substitution through optimized S-boxes and is followed by linear transformation operations that ensure effective diffusion of input variations. SM4 is compatible with several operational modes, including Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and Cipher Feedback (CFB). The ECB mode, as the foundational implementation, processes plaintext in fixed-size blocks (128 bits), encrypting each independently with the same key to produce the corresponding ciphertext blocks. This mode is particularly advantageous for applications requiring independent data blocks due to its simplicity and capability for strong parallel processing. Conversely, the CBC mode increases security through block chaining, while CTR and CFB modes facilitate stream cipher-like functionality, offering adaptability across various application scenarios.

Literature review summary and research gaps

This section summarizes the research gaps in existing literature through a tabular format. Table 1 compares existing research across six key dimensions, revealing the absence of a comprehensive solution. Table 2 provides clear definitions for each dimensional feature, establishing a foundation for the analysis of research gaps.

System design

System overall architecture

The system is designed with a "3 + 1" multi-chain architecture that integrates three business-specific chains along with a cross-chain management platform, promoting secure data exchange and effective collaboration, as illustrated in Fig. 2. The integrated business chains include the production chain, port chain, and sales chain. Each chain is dedicated to specific business operations and maintains data isolation.

Production chain: The production chain caters to manufacturing enterprises and upholds three primary responsibilities: (1) Information Traceability Management: This function entails recording and maintaining crucial production-related information. It includes a comprehensive data trail of production processes, such as product specifications, production batches, sources of raw materials, and quality inspection reports. This

Research	Data security mechanism	Cross-organizational collaboration	Layered data processing	Multi-party data sharing	Cross-chain Interoperability	High concurrency performance
Riazi et al.[4]	×	×	√	×	×	×
Li et al.[6]	×	√	×	√	×	×
Cândido et al.[7]	×	×	×	√	×	×
Giannakis et al.[8]	×	√	×	√	×	×
Selvakumar and Jayashree[9]	×	×	×	×	×	√
Lee and Yeon[10]	√	√	×	×	×	×
Liu et al.[11]	√	×	×	√	×	×
Xue and Wang[12]	√	×	×	×	×	×
Hu et al.[13]	√	×	√	√	√	×
Amico et al.[14]	√	√	×	×	×	×
Xie et al.[15]	√	×	×	×	√	×
Pillai et al.[18]	×	×	×	×	√	√
Xiong et al.[19]	√	×	×	×	√	√
Sun et al.[27]	√	×	×	×	√	×
Proposed system	√	√	√	√	√	√

Table 1. Analysis of literature review and research gaps.

Feature	Description
Data security mechanism	Employs encryption algorithms, access control, and other technologies to ensure data security
Cross-organizational collaboration	Supports business process coordination and data interaction across multiple organizations
Layered data processing	Implements hierarchical management and differentiated protection based on data sensitivity
Multi-party data sharing	Enables secure and efficient data sharing among different participants
Cross-chain interoperability	Facilitates data and value exchange between different blockchain networks
High concurrency performance	Maintains robust system performance in high-concurrency environments

Table 2. Feature descriptions.

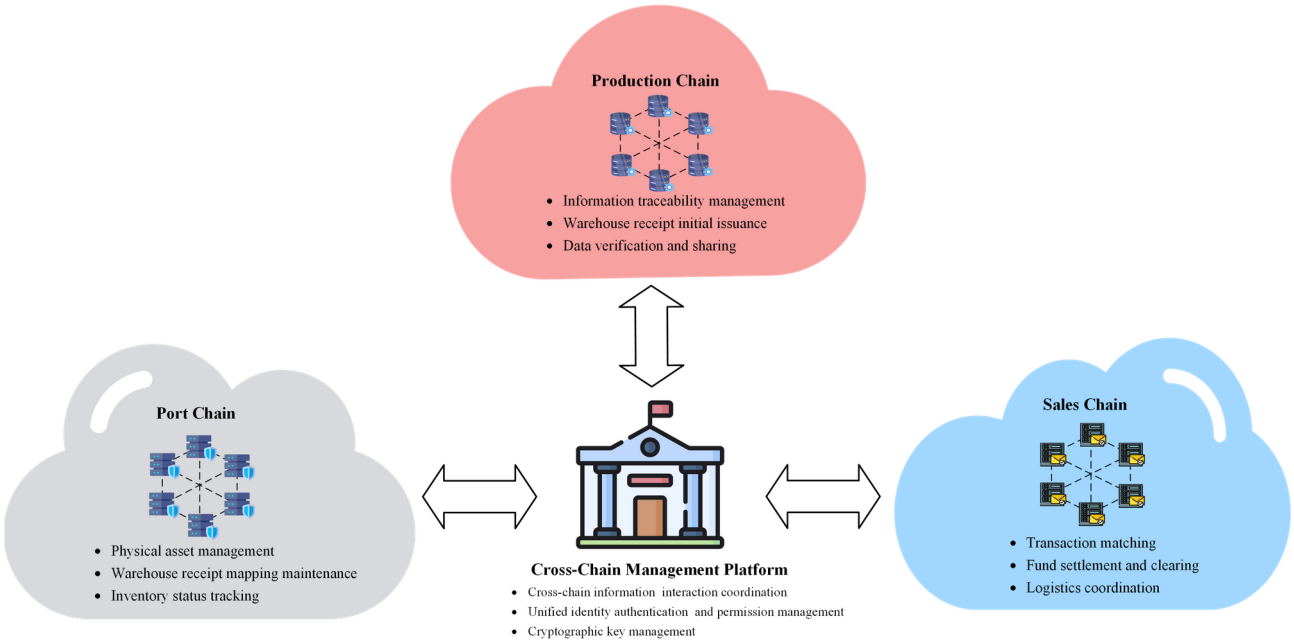

Fig. 2. Overall architecture.

information serves as a reliable foundation for product quality tracing. (2) Warehouse Receipt Initial Issuance: The production chain is tasked with receiving and verifying initial warehouse receipt requests from the port chain. It involves adding detailed production-related information and performing the first issuance after encrypting the data using SM cryptographic algorithms. (3) Data Verification and Sharing: This responsibility involves providing verified production information to other business chains via a cross-chain management platform. It supports the circulation and utilization of warehouse receipts across different business segments.

Port chain: The port chain is dedicated to meeting the operational needs of port enterprises through three core functions: (1) Physical Asset Management: This function manages physical assets during port storage processes, including cargo acceptance, storage, and dispatch. (2) Warehouse Receipt Mapping Maintenance: It ensures a unique mapping between each electronic warehouse receipt and the actual inventory through strict correspondence management, effectively preventing risks such as duplicate warehouse receipts. (3) Inventory Status Tracking: This involves real-time monitoring and updating of cargo storage locations, storage statuses, and other related information, facilitating multi-dimensional, refined inventory management.

Sales chain: The sales chain interfaces with sales enterprises and focuses on three key transaction processes: (1) Transaction Matching: This operation provides a standardized warehouse receipt transaction platform that supports various transaction modes, including spot and forward transactions. (2) Fund Settlement and Clearing: It automates fund-related operations, such as fund transfers and payment confirmations, through smart contracts, thereby reducing settlement risks. (3) Logistics Coordination: This function interfaces with logistics enterprise information systems to manage end-to-end visualization from the completion of the transaction to the delivery of cargo.

Cross-chain management platform: This platform acts as the central hub of the system, managing and coordinating cross-chain functionalities. It performs three critical functions: (1) Cross-Chain Information Interaction Coordination: It operates as a unified platform managing cross-chain communication message queues and routing, ensuring seamless and efficient data exchange between business chains. (2) Unified Identity Authentication and Permission Management: The platform maintains a global registry of participants and implements flexible access control policies, providing a secure and standardized environment for identity verification and data access. (3) Cryptographic Key Management: It is responsible for the generation, distribution,

and rotation of cryptographic keys, utilizing secure algorithms to protect the integrity and confidentiality of inter-chain data transmissions. In contrast to other business chains, the cross-chain management platform does not store specific business data directly. Instead, it operates as a secure control layer that focuses on system-wide operational metadata and security policies.

Main functions

Smart contract-based warehouse receipt management

To enhance the efficiency and transparency of warehouse receipt management within the port supply chain, our system implements a hierarchical smart contract architecture designed to facilitate automated execution of business processes (see Fig. 3). This architecture incorporates a cross-chain management platform equipped with three primary components:

Notary mechanism: This component is responsible for identity authentication and permission control for requests across different blockchain networks.

Data synchronization protocol: It ensures consistency of data across chains through established consensus mechanisms.

Encryption service contract: This works in conjunction with a Key Management System (KMS) and invokes an underlying Hardware Security Module (HSM) to manage cryptographic keys.

Functional contracts, deployed on respective business-oriented blockchain networks, enable automated process execution based on pre-established rules, thereby minimizing the risks associated with manual interventions. The subsequent sections provide a exploration of the operational mechanisms of this smart contract system, with a focus on the processes of generating and transacting warehouse receipts.

To simplify the explanation of warehouse receipt generation and transactions, we focus on the key steps and core logic. For a detailed visual representation, please refer to the flowchart in Fig. 3. The process of warehouse receipt generation can be summarized as follows:

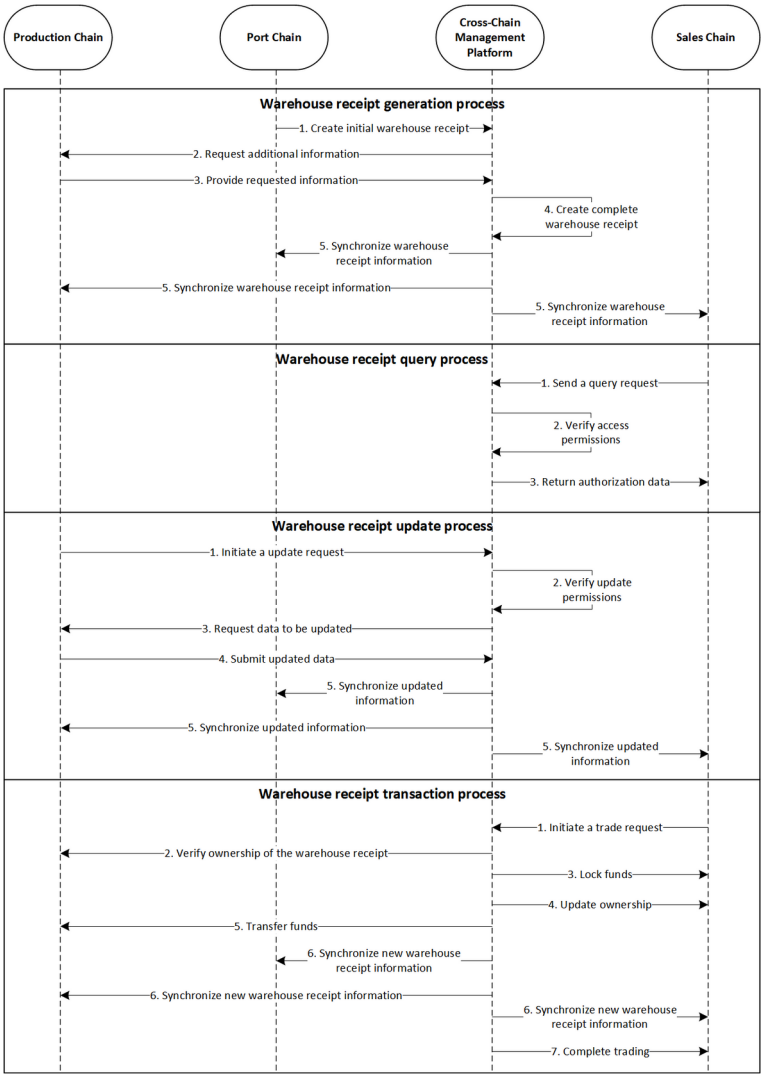

Fig. 3. Business process.

Step 1: Cargo Arrival at the Port: Upon the arrival of the cargo (CARGO_init) at the port, the port enterprise (EP_port) initiates the process by generating the initial warehouse receipt (WR_init). This initial receipt contains basic information about the cargo, such as quantity, type, and origin.

Step 2: Cross-Chain Platform Verification and Forwarding: The port enterprise (EP_port) then submits the generated initial warehouse receipt (WR_init) to the cross-chain management platform (PL_cross) for verification. The platform verifies the authenticity and integrity of the initial warehouse receipt (WR_init) before forwarding it to the original production enterprise (EP_prod).

Step 3: Production Enterprise Enrich Information and Encryption: The production enterprise (EP_prod) enriches the receipt with additional information (e.g., production date, batch number, and quality certification) and encrypts the enriched warehouse receipt using SM encryption algorithms, resulting in a complete warehouse receipt (WR_comp) to ensure data confidentiality.

Step 4: Cross-Chain Platform Verification and Broadcasting: The encrypted warehouse receipt (WR_comp) is submitted again to the cross-chain management platform (PL_cross) for verification. Once successfully verified, the platform broadcasts the warehouse receipt to other relevant business chains, allowing authorized stakeholders to access it.

After the warehouse receipt is generated, the transaction process can be summarized as follows:

Step 1: Buyer Initiation: The buyer enterprise (EP_buy) initiates the transaction process by making a payment request on the sales chain (CH_sale).

Step 2: Cross-Chain Platform Verification: The buyer enterprise (EP_buy) submits the transaction request to the cross-chain management platform (PL_cross). The platform verifies the buyer's credentials and ensures that the transaction complies with predefined rules and regulations.

Step 3: Warehouse Receipt Transfer and Ownership Update: After successful verification, the cross-chain management platform (PL_cross) facilitates the transfer of the warehouse receipt (WR_comp) from the seller enterprise (EP_sell) to the buyer enterprise (EP_buy). This transfer involves updating the ownership records on all blockchains, ensuring a transparent and immutable record of the transaction.

Step 4: Confirmation and Settlement: After the warehouse receipt (WR_comp) has been transferred, both the buyer enterprise (EP_buy) and the seller enterprise (EP_sell) receive transaction confirmation. The two parties can then execute the transaction settlement using the payment mechanism predefined in the smart contract.

Notary mechanism-based cross-chain communication

Cross-chain communication plays a pivotal role in facilitating data sharing and business coordination within a multi-chain architecture. Our system utilizes a notary mechanism-based approach for cross-chain communication, which orchestrates a star topology centered around the cross-chain management platform (see Fig. 4). This configuration effectively supports the transmission and synchronization of information across different business chains, ensuring secure, accurate, and efficient data handling during the generation, query, update, and transaction phases of warehouse receipt management.

In the cross-chain communication process, the core working mode of the notary mechanism (distributed collaboration of notary nodes) is as follows:

The notary mechanism implements decentralized trust verification through a network of selected notary nodes. The cross-chain management platform (PL_cross) selects trusted institutions (e.g., customs regulators, banks, large logistics companies) as notary nodes from business chains such as the port chain (CH_port), production chain (CH_prod), and sales chain (CH_sale), ensuring the geographical distribution of nodes and the diversity of business roles.

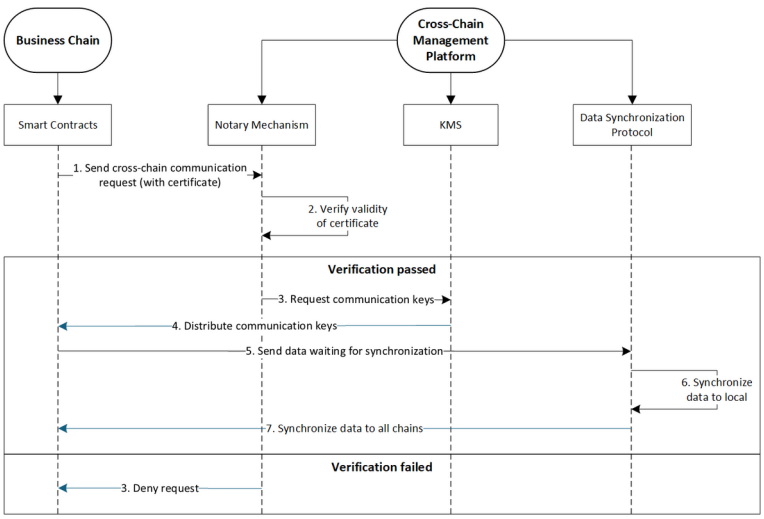

Fig. 4. Cross-chain communication process.

When a production chain node (EP_prod) initiates a cross-chain warehouse receipt update request (REQ_cross), the notary mechanism operates according to the following process:

Identity and permission verification: The first notary node (PN_1) to receive the request invokes an on-chain verification smart contract (CONTRACT_verify), using the SM2 public-key decryption algorithm to parse the requester's digital certificate (CERT_prod), confirming its legitimacy and operational permissions (e.g., the warehouse receipt update permission must match the role code EP_prod).

Multi-Node Byzantine consensus: After successful verification, PN_1 broadcasts the request to all notary nodes in the network, which then perform multiple rounds of voting based on the improved Byzantine Fault Tolerance protocol (BFT+). The protocol sets a valid consensus threshold of $N\_valid \geq 2\ N/3$ (where N is the total number of nodes). Only when more than the threshold of notary nodes confirm the legitimacy of the request can the cross-chain operation be triggered.

Using the process of generating warehouse receipts and their cross-chain communication as an illustrative example, the detailed steps can be described as follows:

Step 1: When the production chain (CH_prod) requires interaction with the port chain (CH_port), the production enterprise (EP_prod) initiates a cross-chain request (REQ_cross). This request includes the identifier for the target chain (CH_port), the type of operation (e.g., updating warehouse receipt information), and the data payload. The production enterprise (EP_prod) then signs the request using its private key (KEY_priv_prod), attaches the signature and its digital certificate (CERT_prod) registered on the cross-chain management platform (PL_cross), and dispatches the complete request to the platform (PL_cross).

Step 2: Upon receipt of REQ_cross, the notary node (PN_1) on the cross-chain management platform (PL_cross) activates a verification contract (CONTRACT_verify) to conduct several checks: it validates the legitimacy of EP_prod's identity using CERT_prod, examines EP_prod's access permissions for the targeted data, and confirms the validity of the request's signature.

Step 3: Following successful verification, notary node (PN_1) establishes a secure communication channel (CHANNEL_sec) between the cross-chain management platform (PL_cross) and the port chain (CH_port). This channel employs the SM2 encryption algorithm to safeguard the data during transmission.

Step 4: With the established secure channel (CHANNEL_sec), the production enterprise (EP_prod) on the production chain (CH_prod) and the port enterprise (EP_port) on the port chain (CH_port) can directly perform secure data transmission and interaction, realizing the update and sharing of cross-chain data. After receiving and verifying the data, EP_port stores it in the local ledger and directly feeds back the processing results to EP_prod through this secure channel, completing this cross chain communication.

Data layering and SM cryptographic algorithm-based encryption scheme

To effectively manage the diversity and varying sensitivity of data within port supply chains, the system implements a differentiated encryption strategy using SM cryptographic algorithms, which integrates a layered data structure to strike a balance between data security and sharing efficiency. The data is divided into four different levels, and the specific hierarchical structure is shown in Table 3.

The system adopts a tiered encryption strategy tailored to different data sensitivity levels, utilizing SM cryptographic algorithms. Unencrypted data is retained for basic information due to efficiency considerations. Moderately sensitive data is protected using the SM4-ECB symmetric encryption algorithm in conjunction with group keys, thus enabling decryption exclusively by authorized group members. For instance, port enterprises and insurance companies may collaborate as a group to exchange information related to storage fees and insurance. Group keys are created and overseen by a group administrator, encrypted with SM2 for distribution to group members, and are subsequently updated and reissued following any changes in group composition. Highly sensitive data is secured using distinct SM4-ECB keys for each critical information field, which assures that the compromise of one key does not jeopardize the security of other fields. Access to these keys is restricted to participants who possess specific permissions. For example, a warehouse receipt owner may have access to the keys for all fields, whereas transaction parties may only access keys pertinent to transaction data relevant to them. Information pertaining to version control remains unencrypted. Additionally, the SM3 algorithm is employed to compute and store hash values for all data to ensure integrity.

The system's data processing workflow is comprehensive, addressing data stratification and encryption. Upon receiving warehouse receipt data, DATA_wr, from a production enterprise, EP_prod, the system methodically divides the information into four principal layers: the base layer, LAYER_base, contains essential attribute information; the business layer, LAYER_biz, includes moderately sensitive data; the core layer, LAYER_core, encompasses highly sensitive data; and the control layer, LAYER_ctrl, maintains version control data.

Data layer	Included fields	Access permissions	Encryption strategy
Basic information	Variety, quantity, quality, specifications, origin, cargo ID, weight, volume, etc.	Public	\
Moderately sensitive information	Storage fees, insurance status, transportation methods, estimated arrival time, etc.	Authorized	SM4-ECB symmetric encryption, group keys
Highly sensitive information	Ownership information, transaction prices, transaction party identities, transaction records, etc.	Restricted	SM4-ECB symmetric encryption, independent keys for each field
Version control information	Version number, timestamp, data hash value, etc.	Public	\

Table 3. Warehouse receipt data layering.

Differentiated encryption strategies are applied across these layers. Data in LAYER_base, such as initial cargo attributes CARGO_init, remains unencrypted to enhance processing efficiency. LAYER_biz uses group-based encryption facilitated by the SM4-ECB algorithm, resulting in the ciphertext ENC_biz. Here, the business group, GROUP_biz, shares a communal key, KEY_group, for accessing data. LAYER_core implements field-level encryption, where individual sensitive fields like ownership information, INF_owner, and transaction records, INF_transact, are encrypted with separate SM4-ECB keys (KEY_owner and KEY_transact respectively), producing the corresponding ciphertexts (ENC_owner and ENC_transact). To uphold the integrity of data across all layers, the key management system, KMS_sys, calculates a combined hash value, HASH_all, using the SM3 algorithm, which is then stored in LAYER_ctrl.

The KMS_sys, deployed on the cross-chain management platform PL_cross, orchestrates key distribution, managing both the KEY_group for GROUP_biz members and field-specific keys (KEY_owner and KEY_transact) for authorized enterprises EP_prod and EP_port. When there are changes in the membership of GROUP_biz, such as the addition of a new enterprise EP_new, KMS_sys automatically initiates a key update sequence. This sequence entails the generation of a new group key, KEY_group_new, using the SM2 algorithm to ensure secure distribution among updated group members, followed by the re-encryption of pertinent business layer data to produce a new ciphertext, ENC_biz_new. Subsequently, the system synchronizes ENC_biz_new and key distribution information across all relevant business chains, thereby maintaining consistent security throughout the network.

Key management is conducted through KMS on the cross-chain management platform, offering comprehensive lifecycle key management services within a multi-layer security architecture underpinned by HSM. In terms of system implementation, key storage utilizes HSM for hardware-level protection, while the key transmission processes establish secure channels through SM2 asymmetric encryption, supplemented by PKI digital certificate mechanisms, and implement role-based fine-grained access control. For data protection, the system employs the SM4-ECB algorithm for encryption to safeguard data confidentiality, utilizes the SM2 algorithm for reliable identity authentication and key distribution, and leverages the SM3 algorithm to calculate data hash values, ensuring data integrity. This KMS-based key management mechanism provides robust assurance for data security and flexible sharing within port supply chains.

Through the above-mentioned data layering and encryption mechanisms, proposed system aims to build a secure and reliable warehouse receipt management platform. To comprehensively present the internal logic of this security system, a deeper analysis of the SM cryptographic algorithms used is provided below:

SM4-ECB symmetric encryption algorithm: This algorithm offers efficient encryption and decryption speeds, making it suitable for large-scale data encryption. In the business and core layers, we chose the SM4-ECB algorithm because it provides a high processing efficiency while ensuring a certain level of security strength. Although the ECB mode has some security vulnerabilities, in this system, we effectively mitigate the risks of ECB mode through strict key management and access control measures, as well as its coordination with other security mechanisms. In the future, we will consider introducing more secure encryption modes (such as CBC, CTR, etc.) to further enhance the system's security.

SM2 asymmetric encryption algorithm: This algorithm offers high security and is suitable for key management and identity authentication scenarios. In this system, we use the SM2 algorithm to encrypt group keys (KEY_group) and field keys (KEY_field) to ensure the security of keys during transmission and storage. Additionally, the SM2 algorithm is used to verify the identities of participants, preventing unauthorized access. Although the SM2 algorithm has longer key lengths and higher computational complexity, its security is sufficient to meet the needs of this system.

SM3 hash algorithm: This algorithm has good collision resistance and one-way properties, making it suitable for data integrity verification. In this system, we use the SM3 algorithm to compute the hash value (HASH_all) of data, which is stored in the control layer (LAYER_ctrl) to verify the integrity of the data. Any tampering with the data will cause the hash value to change, which will be detected by the system. The SM3 algorithm has a fast computation speed and can meet the real-time requirements for data integrity verification in the system.

Optimization strategies

To further enhance system performance, the following optimization strategies have been implemented:

1. Batch processing.

In traditional cross-chain interactions, the independent verification and transmission of individual requests can lead to significant communication and computation overhead. To address this, proposed system introduces a dynamic batch processing mechanism. The core idea is to aggregate multiple related requests (e.g., warehouse receipt query requests REQ_1, REQ_2, REQ_3 from the same enterprise EP_prod) into a single transaction batch (BATCH_prod) and optimize it through the following steps:

Request classification and merging: Cross-chain requests are dynamically grouped based on request type (such as query or update), initiator identity, and target chain information. For instance, multiple warehouse receipt status query requests from the same enterprise can be merged into a single batch.

Batch verification and signing: All requests within the batch undergo unified identity authentication and permission verification, and batch signing by notary nodes is used to reduce the number of cryptographic operations.

Cross-Chain communication protocol optimization: A lightweight serialization protocol (such as Protocol Buffers) is employed to compress and encode the batch data, reducing the network transmission volume. Additionally, dynamic timeout thresholds are set to balance throughput and real-time demands, enabling more efficient cross-chain communication.

2. Incremental synchronization.

To address the issue of cross-chain synchronization efficiency caused by frequent warehouse receipt data updates, proposed system designs an incremental synchronization mechanism based on version control. The key technologies include:

Field-Level difference detection: By comparing the current state of the warehouse receipt (WR_curr) with the previous version (WR_prev), only the changed fields (FIELD_new) are extracted to generate an incremental data packet (Δ_WR). For example, if the weight of the goods recorded on the warehouse receipt changes from 100 tons to 120 tons, only the weight field, rather than the entire warehouse receipt record, is synchronized.

Version chain management: A hash chain (Hash_Chain) is maintained for each warehouse receipt, recording timestamps of historical versions, updated abstracts, and signatures of notary nodes to ensure data traceability and immutability.

Adaptive Synchronization Trigger: Synchronization triggers are set based on the business scenario: high-priority operations (e.g., warehouse receipt pledge) are synchronized in real-time, while low-priority operations (e.g., log updates) are synchronized periodically in batches. This strategy aims to significantly reduce cross-chain data traffic while ensuring the real-time nature of critical operations.

3. Parallel processing.

To achieve efficient processing in high-concurrency scenarios, proposed system constructs a parallel execution engine based on Directed Acyclic Graph (DAG). The workflow is as follows:

Operation dependency analysis: Static code analysis and runtime monitoring are used to identify data dependencies between operations in the smart contract (e.g., OP_1, OP_2). For example, the warehouse receipt ownership transfer (OP_transfer) must wait for the pledge status confirmation (OP_pledge), while logistics information update (OP_logistics) can be executed independently.

Task parallel scheduling: Operations without dependencies are assigned to different threads or containers for parallel execution, and lightweight locking mechanisms (Fine-grained Locking) are employed to avoid resource contention. This framework is designed to make full use of system resources and enhance transaction processing efficiency.

Result consistency assurance: The two-phase commit protocol (2PC) is used to atomically commit the results of parallel operations, ensuring the eventual consistency of cross-chain transactions. If any operation fails, the system automatically triggers a compensation transaction to perform a rollback.

Experiments and analysis

Configuration

The system deploys production chain, port chain, sales chain, and cross-chain management platform on four separate virtual machines, with each chain running on an independent virtual machine to achieve physical isolation. Detailed configurations are shown in Tables 4 and 5.

Performance evaluation

The evaluation of the system's performance is structured around three key dimensions: computational capability, responsiveness, and reliability.

Computational capability: The principal metric for assessing computational capability is transaction throughput, which is further divided into query throughput and transaction throughput. These sub-indicators are designed to capture the system's performance characteristics under varying business loads.

Responsiveness: System latency is the primary metric for this dimension, defined as the time interval between the initiation of a request and the completion of the response. This measure provides a quantitative basis for evaluating the performance of the cross-chain architecture.

Reliability: The operation success rate is utilized as an auxiliary measure to gauge system stability under conditions of high concurrency and to document performance degradation characteristics.

The experimental design adheres to the ISO/TC 307 standards for blockchain systems. A progressive load testing methodology was employed, consisting of three phases:

- Baseline performance evaluation for 400–800 concurrent users.
- Peak processing capability assessment for 800–1000 concurrent users.
- Performance limit exploration for 1000–1400 concurrent users.

To ensure the integrity of the data, each test iteration was performed 1000 times, using statistical methods to mitigate the impact of random variations.

Item	Configuration	URL
CPU	Intel Core i7-14700 H	\
Memory	64GB	\
Storage	2 TB SSD	\
Operating system	Ubuntu 20.04 LTS	https://releases.ubuntu.com/20.04/

Table 4. Experimental environment.

Item	Configuration		URL
	Business chains	Cross-chain management platform	
Blockchain platform	Hyperledger Fabric 2.4.9	Hyperledger Fabric 2.4.9	https://hyperledger-fabric.readthedocs.io/en/release-2.4/
Container engine	Docker Engine 27.3.1	Docker Engine 27.3.1	https://docs.docker.com/engine/release-notes/27/#273
Smart contract language	Go 1.22.1	Go 1.22.1	https://go.dev/doc/go1.22
Application layer development	Node.js 22.13.0	Node.js 22.13.0	https://nodejs.org/en/blog/release/v22.13.0
Testing tool	Hyperledger Caliper 0.5.0	Hyperledger Caliper 0.5.0	https://github.com/hyperledger-caliper/caliper/releases/tag/v0.5.0
CPU cores	4 cores	4 cores	\
Memory	8GB	8GB	\
Storage	50GB SSD	50GB SSD	\
Number of nodes	3	4	\

Table 5. Virtual machine environment.

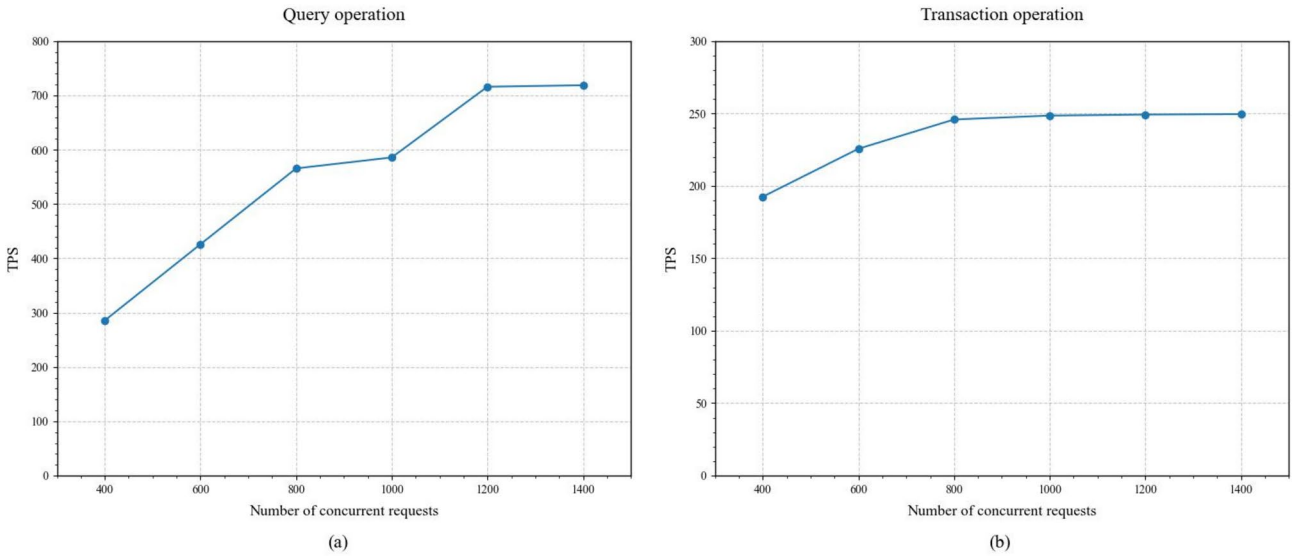

Fig. 5. Throughput versus concurrency in different operations.

Blockchain

Utilizing the recognized Hyperledger Caliper (v0.5.0) as a testing tool, the paper assessed three critical performance indicators—throughput, latency, and success rate—across different levels of user concurrency (400–1400 users). The tests simulated realistic business operations, encompassing both query and transaction processes.

1. Throughput.

The throughput results, depicted in Fig. 5, show that for query operations, system throughput displays a logarithmic growth pattern as the number of concurrent users increases, stabilizing at approximately 720TPS at 1400 users. This growth trajectory is largely influenced by the system's layered data structure and the efficiencies introduced by optimized query mechanisms. Notably, at user levels below 800, the query throughput exhibits significant linear growth, increasing from 285.5TPS to 565.4TPS—a 98.0% increase. This enhancement is primarily attributed to the effective parallel processing mechanisms implemented within the system. However, as the user load continues to rise, the rate of performance improvement moderates, primarily due to the increasing overhead from cross-chain communications, which imposes constraints on the overall system performance.

In contrast, transaction operations exhibit markedly distinct performance characteristics. In low-load environments, defined as 400 to 800 concurrent users, transaction throughput experiences a moderate increase from 182.5TPS to 245.8TPS, reflecting a relatively gentle growth trend with a rate of increase (34.7%) significantly lower than that observed in query operations during the same timeframe. This disparity in performance primarily arises from the inherent complexities associated with transaction operations, which

include additional computational demands due to multiple verification stages in cross-chain consensus processes and data synchronization tasks. In high-load scenarios, ranging from 1000 to 1400 concurrent users, the growth in transaction throughput further moderates, ultimately stabilizing at approximately 250TPS. This stabilization suggests that the system retains robust transaction processing capabilities even under conditions of high concurrency.

2. Latency.

The performance evaluation concerning latency of different operations (refer to Fig. 6) shows that query operations exhibit exceptionally stable latency characteristics. In environments with low user concurrency (400–800 users), the system's average latency increases only marginally, from 245.6ms to 485.3ms, underscoring the system's high performance stability. As the number of concurrent users rises to 1000, latency displays a gradual linear growth, reaching 552.8ms, with the rate of increase remaining within a reasonable margin. Notably, even in extreme load scenarios (1000–1400 concurrent users), the growth in system latency remains effectively managed, with an increase from 552.8ms to 598.5ms (8.3% increase), which vividly demonstrates the system's robust stability under significant stress. This superior latency performance largely derives from the system's implementation of a layered data management architecture and optimized query strategies. The layered data structure significantly diminishes data access complexity, while optimized query strategies effectively shorten response times through parallel processing mechanisms.

In contrast, transaction operations display distinctly different latency characteristics and growth patterns. In low-load environments (400–800 concurrent users), the average system latency escalates from 3325.6ms to 4885.3ms, indicating a relatively high baseline latency level. As the number of concurrent users increases, the growth in latency exhibits notable non-linear characteristics: in medium-load intervals (800–1000 users), system latency further escalates to 5285.6ms, marking an increase of 8.2%; while in high-load scenarios (1000–1400 users), although latency continues to rise, reaching 5485.4ms, the rate of increase notably decelerates to merely 3.8%. This intricate latency performance directly reflects the substantial overhead introduced by cross-chain consensus mechanisms and the multiple verification processes essential to transaction operations. Particularly in high-concurrency environments, the complexity of cross-chain interactions and the temporal overhead associated with consensus processes become critical factors impacting system performance. Nevertheless, even under considerable processing pressure, the system maintains latency increases within acceptable limits, thereby fully validating the feasibility and effectiveness of the proposed cross-chain architecture in practical application scenarios.

3. Success rate.

The analysis of the system's operational reliability reveals substantial technical benefits. In extensive performance evaluations, the system demonstrates exceptional operational stability. It maintains a 100% success rate in query and transaction operations, even under varying loads—from a baseline of 400 concurrent users to extreme scenarios of 1400 concurrent users. This performance metric is crucial for two reasons: Firstly, it confirms the efficacy of the notary mechanism-based cross-chain solution in ensuring operational reliability. Even in high-concurrency environments, where the system endures significant performance stresses (with query latency reaching 598.5ms and transaction latency peaking at 5485.4ms), it consistently executes all operations accurately. This underscores the notary mechanism's role in preserving the consistency of cross-chain operations. Secondly, unlike traditional centralized systems, which frequently encounter operation failures or timeouts under high

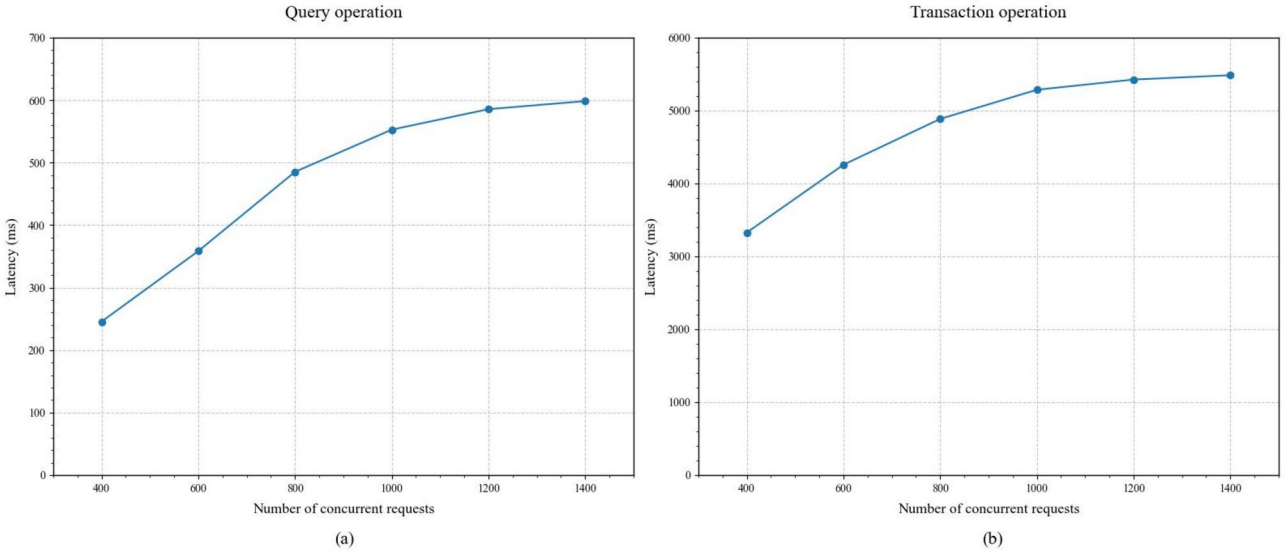

Fig. 6. Latency versus concurrency in different operations.

stress, the robust reliability of this system provides a reliable foundation for stable operation in real-world business contexts.

4. Indicator correlation.

Through methodical experimentation and detailed analysis, this paper uncovers the inherent correlations between key performance indicators—throughput and latency—of the system under review. Statistical examination of a substantial dataset (1000 repetitions per test group) highlights discernible performance disparities between query and transaction operations. These differences are consistent and reproducible, clearly delineating the distinct performance characteristics inherent to each operation type.

Further in-depth analysis of these performance metrics (as illustrated in Fig. 7) identifies a significant non-linear relationship between system latency and throughput. For query operations, a marked performance trade-off becomes apparent when concurrent user numbers exceed 1000. During this interval, query latency increases from 552.8ms to 598.5ms—an 8.3% rise—while throughput sees a modest enhancement from 685.6TPS to 718.5TPS, an increase of 4.8%. This behavior is closely linked to the system's batch processing mechanism, which manages resource utilization by strategically delaying certain requests to stabilize overall throughput.

For transaction operations, the latency-throughput relationship is more complex. Data shows that with fewer than 800 concurrent users, the system scales effectively: transaction throughput increases by 34.7%, from 182.5TPS to 245.8TPS, while latency escalates by 46.9%, from 3325.6ms to 4885.3ms, demonstrating a relatively linear growth pattern. Beyond this threshold, particularly after reaching 1000 concurrent users, the performance curve displays a notable inflection point: transaction latency marginally rises from 5285.6ms to 5485.4ms (a 3.8% increase), while throughput remains nearly constant with a 0.4% increase. This observation indicates that the system, even under substantial loads, maintains a relatively stable performance, thereby affirming the scalability and robustness of the proposed cross-chain architecture.

Cryptographic algorithm

This section evaluates the performance of the differentiated encryption strategy implemented by the system through comprehensive performance testing of various cryptographic algorithms across multiple data scales. Given the typical data size characteristics of warehouse receipts within practical port supply chain scenarios, the data scale for testing was set at 50KB, 200KB, 1 MB, and 5 MB, with a focus on two primary metrics: the execution time and the throughput of encryption and decryption operations.

As illustrated in Fig. 8, the test results elucidate the performance traits of three categories of cryptographic algorithms across varying data scales. In the case of asymmetric encryption algorithms, the execution time for the SM2 algorithm increases significantly as the data scale expands. For instance, the encryption and decryption times for 50KB of data are 145.3ms and 98.5ms, respectively, which escalate to 15,325.6ms and 10,385.4ms for 5 MB of data. Conversely, the SM4-ECB symmetric encryption algorithm displays markedly superior performance, requiring only 42.5ms for encrypting and 37.8ms for decrypting 50KB of data, with times increasing to 4,425.3ms and 3,885.6ms for 5 MB of data, reflecting a more moderate growth in execution time. The SM3 hash algorithm exhibits the most efficient performance and scalability, with processing times rising from just 26.0ms for 50KB to 2,685.3ms for 5 MB of data, demonstrating an excellent linear scaling attribute.

In terms of throughput, each algorithm displays distinct performance characteristics. The SM2 algorithm records encryption and decryption throughputs of 347.1KB/s and 507.6KB/s, respectively, for 50KB data. These rates slightly decrease to 315.7KB/s and 480.5KB/s when processing 5 MB data. The SM4-ECB algorithm

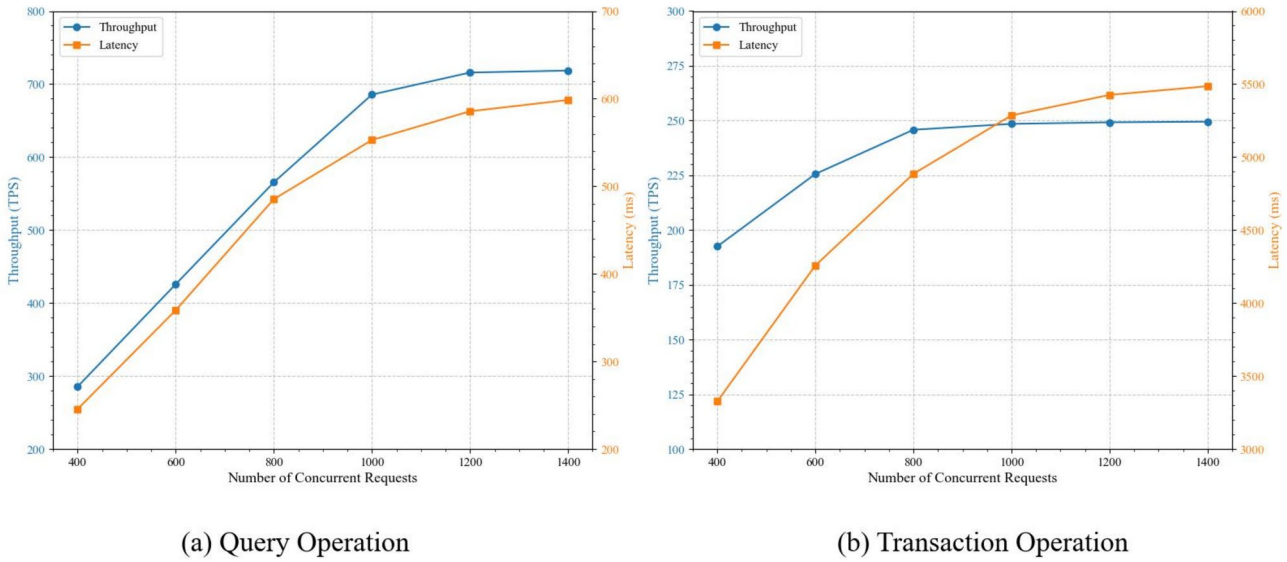

Fig. 7. Relationship between throughput and latency in different operations.

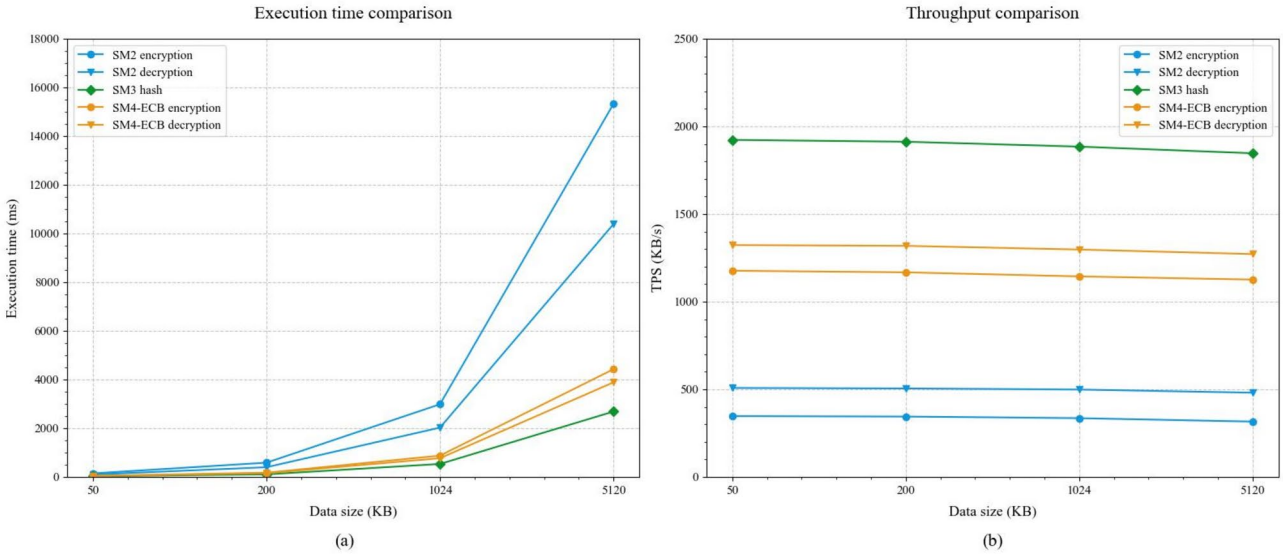

Fig. 8. Performance of different cryptographic algorithms.

consistently maintains high throughput, exceeding 1100KB/s for all tested data scales. Specifically, it achieves encryption and decryption throughputs of 1176.5KB/s and 1322.8KB/s for 50KB data, sustaining 1125.8KB/s and 1271.6KB/s even with 5 MB data. The SM3 algorithm demonstrates optimal throughput performance, maintaining over 1800KB/s across all test data scales with minimal performance degradation, ranging from 1923.1KB/s at 50KB to 1846.7KB/s at 5 MB.

The multi-scale test results affirm that the system's differentiated encryption strategy sustains robust performance across various data scales. For the verification of integrity at the basic information layer, the performance-optimized SM3 algorithm effectively supports the rapid processing of large-scale data. For the encryption requirements of business and core information layers, the SM4-ECB algorithm provides stable, high performance across diverse data scales, whether it is utilized for group keys in business information or independent field-level keys for core sensitive data. Additionally, although the SM2 algorithm exhibits comparatively lower performance with larger data volumes, it remains adequately suited for secure key distribution and identity authentication tasks, supporting these specific security operations effectively.

These differentiated performance characteristics are well-aligned with the system's layered encryption strategy, thereby ensuring overall processing efficiency while maintaining robust data security. The test results not only validate the rationality of the current encryption strategy but also provide crucial performance benchmarks for future system optimization and expansion.

Comparative analysis

Cryptographic algorithms

To rigorously assess the efficacy of the cryptographic algorithms implemented within the system, this section conducts a comparative analysis between the SM cryptographic algorithms (SM2, SM3, SM4) and internationally recognized cryptographic algorithms (RSA, SHA-256, AES). The evaluation, based on experiments conducted within the standardized environment delineated in Table 4, focuses on two pivotal metrics: encryption and decryption times, and throughput. The assessment spans four distinct data sizes—50KB, 200KB, 1 MB, and 5 MB—to ascertain performance in varied practical business contexts.

The experimental outcomes, as illustrated in Fig. 9, provide a thorough examination of the performance distinctions between the SM suite and global cryptographic standards across varying data volumes. In the realm of asymmetric encryption, SM2 exhibits substantial efficiency advantages over RSA. For instance, at the 50KB data level, SM2 requires 145.3ms for encryption and 98.5ms for decryption, achieving throughputs of 347.1KB/s and 507.6KB/s, respectively. In contrast, RSA necessitates 165.8ms for encryption and 112.4ms for decryption, with corresponding throughputs of 301.6KB/s and 444.8KB/s. As data volumes escalate to 5 MB, the performance disparity becomes more marked: SM2 records encryption and decryption times of 15,325.6ms and 10,385.4ms (yielding throughputs of 315.7KB/s and 480.5KB/s, respectively), compared to RSA's times of 17,568.4ms and 11,925.8ms (with throughputs of 283.3KB/s and 419.2KB/s). This represents a performance enhancement of approximately 13.0%, predominantly attributable to the elliptic curve cryptography employed by SM2, which substantially reduces computational demands while maintaining comparable security efficacy to RSA's factorization-based algorithm.

In the evaluation of hash algorithms, SM3 and SHA-256 demonstrate distinct performance metrics. When processing 50KB of data, SM3 completes in 26.0ms, reaching a throughput of 1923.1KB/s, whereas SHA-256 takes 28.5ms, with a throughput of 1754.4KB/s. As data size increases to 5 MB, the divergence in performance between the two algorithms becomes more pronounced: SM3 operates in 2685.3ms, maintaining a throughput

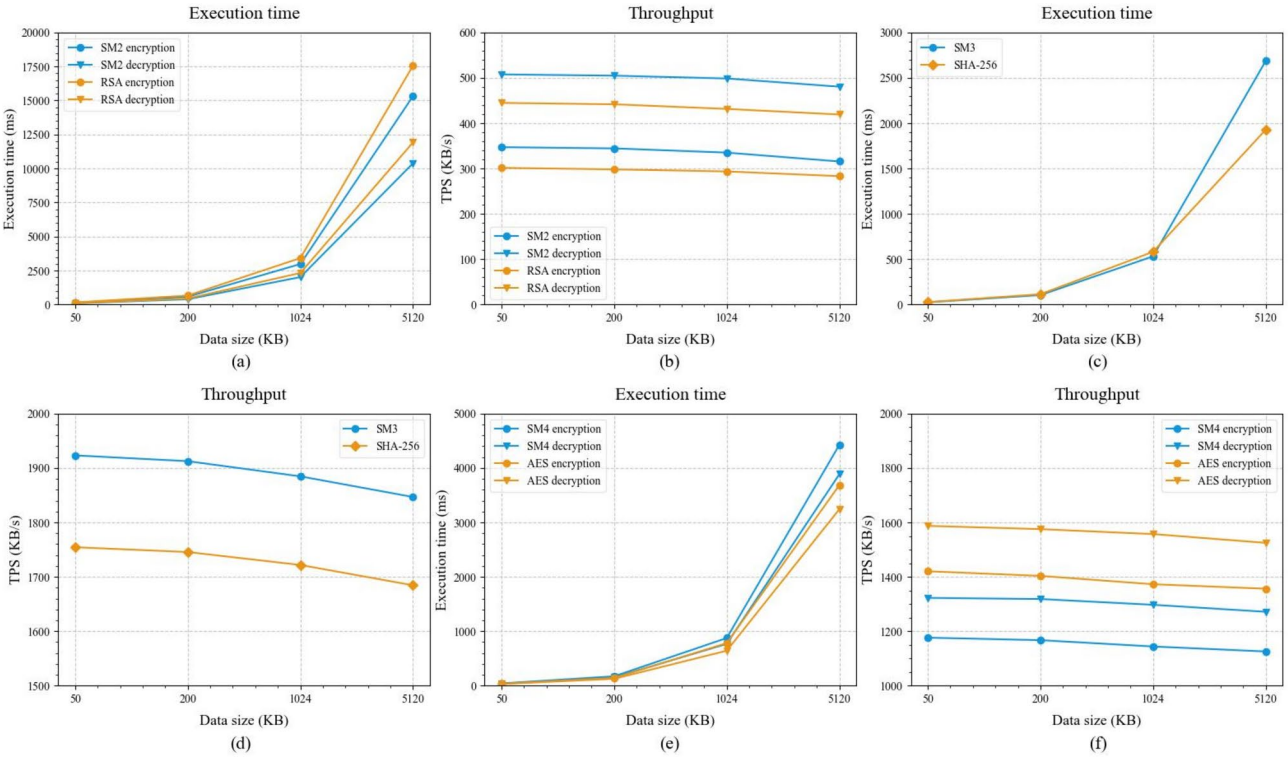

Fig. 9. Performance comparison of different cryptographic algorithms.

of 1846.7KB/s, while SHA-256's time increases to 2928.5ms, with its throughput reducing to 1684.5KB/s. This trend underscores SM3's superior scalability and stability in handling larger data volumes.

The comparative testing of symmetric encryption algorithms reveals similar performance trends between SM4-ECB and AES-ECB. With 50KB of data, SM4-ECB achieves encryption and decryption times of 42.5ms and 37.8ms, respectively, with throughputs of 1176.5KB/s and 1322.8KB/s, showcasing efficient processing capabilities. In comparison, AES-ECB records encryption and decryption times of 35.2ms and 31.5ms, respectively, with throughputs of 1420.5KB/s and 1587.3KB/s. As data volume increases to 5 MB, both algorithms maintain robust performance: SM4-ECB with encryption and decryption times of 4425.3ms and 3885.6ms (and throughputs of 1125.8KB/s and 1271.6KB/s, respectively), and AES-ECB with times of 3685.4ms and 3242.5ms (and throughputs of 1356.4KB/s and 1524.8KB/s). These results confirm the stability of both algorithms across diverse data scales.

An in-depth analysis of experimental data reveals that within standard software environments, the SM cryptographic algorithm family (comprising SM2, SM3, and SM4) exhibits distinct performance characteristics when compared to international cryptographic standards. Particularly, in the domains of asymmetric encryption and hash computation, SM2 and SM3 show clear advantages over RSA and SHA-256, respectively. Conversely, in the realm of symmetric encryption, SM4-ECB and AES-ECB demonstrate stable and comparable performance levels. These observations underscore the specialized optimizations achieved by SM cryptographic algorithms in asymmetric encryption and hash computation, while highlighting that both SM4-ECB and the internationally recognized AES-ECB maintain high performance standards in symmetric encryption. Notably, performance enhancements are achievable for both algorithms on modern processors equipped with hardware acceleration instruction sets.

These findings serve as crucial reference points for algorithm selection across various application contexts. For instance, within resource-constrained embedded systems, SM cryptographic algorithms, which excel in asymmetric encryption and hash computation, may be favored. Conversely, in server environments, both SM4-ECB and AES-ECB offer reliable performance assurances for symmetric encryption tasks. Additionally, these experimental outcomes support the rationality behind adopting a differentiated encryption strategy within systems. This strategy involves selectively employing the most suitable encryption algorithm based on specific application scenarios, levels of data sensitivity, and characteristics of the hardware environment. Ultimately, this approach facilitates an optimal balance between security and performance.

Blockchain systems

To evaluate the advancements in system performance, this paper has chosen the Hyperledger Fabric-based port supply chain system developed by Gao et al.[22] as the benchmark. This system epitomizes the prevailing technological strategies in blockchain applications for port supply chains by employing a single-chain architecture to manage core business processes, such as access control policy development, cargo document handling, and order inquiries. At the level of data management, it consolidates the storage of all participant

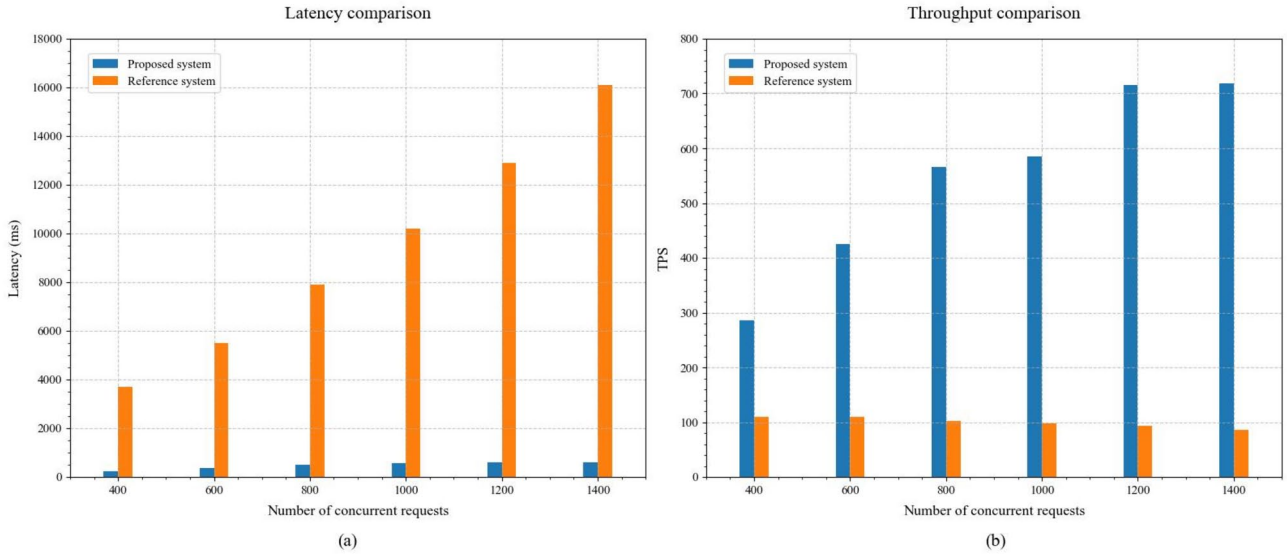

Fig. 10. Performance comparison of different systems in query operation.

data within a single blockchain, while controlling access through a Role-Based Access Control (RBAC) mechanism. For cross-organizational data exchanges, the system utilizes a conventional request-response method, mandating that all operational requests undergo verification via centralized authentication services. Although this architectural choice simplifies implementation, it introduces inherent limitations concerning data segregation, privacy safeguards, and the handling of high-concurrency transactions. Given the distinctions in business-specific functionalities between the two systems, this research utilizes query operations as the primary metric for performance comparison. This decision is grounded on several factors: firstly, query operations are critical as they directly influence the efficiency of data retrieval and access management within blockchain systems; secondly, given their broad applicability and comparability, query operations serve as a valuable benchmark for evaluating the performance of systems with differing architectural configurations; and lastly, in practical scenarios within port supply chains, the effectiveness of query operations substantially impacts the response time for business processing and overall user experience, thereby playing a crucial role in the system's operational value. To secure dependable performance metrics, this investigation executed a series of system performance tests within a predefined hardware setup (referenced in Tables 2 and 3). These tests spanned various levels of concurrent user loads, ranging from 400 to 1400, with each testing group undergoing 1000 repetitions to guarantee statistical validity. For the system used as a reference, performance metrics for the user range from 400 to 1000 were estimated by analyzing graphical data from their published findings, and projections for the 1000–1400 user range were made based on observed performance trends. Although this method of comparison has its limitations, the significant and statistically relevant differences in performance under comparable loads between the two systems provide substantial evidence supporting the superior performance of the proposed system.

As depicted in Fig. 10(a), the experimental results for performance comparison highlight the significant advantages of the proposed system in terms of query response times. In environments with low user concurrency (400 concurrent users), the proposed system achieves an average response time of only 245.6ms, compared to the reference system's 3700ms; this disparity in performance becomes even more pronounced as the load increases. When the number of concurrent users rises to 800, the proposed system maintains its response time within a manageable 485.3ms, whereas the response time for the reference system soars to 7900ms. In scenarios of extreme load (1400 concurrent users), the proposed system continues to keep its response time at a low 598.5ms, while the response time for the reference system escalates to 16100ms.

Regarding system throughput, the experimental data also underscore the exceptional performance of the proposed system (as illustrated in Fig. 10b). In the low-load range (400–800 users), the throughput of the proposed system steadily increases from 285.5TPS to 565.4TPS; meanwhile, the throughput of the reference system remains approximately constant at 100TPS, showing a declining trend as the load increases. In the medium-load range (800–1000 users), the throughput of the proposed system continues to rise, reaching 685.6TPS, which highlights its robust capacity for concurrent processing. In stark contrast, the throughput of the reference system diminishes to 98TPS. Most notably, even in the high-load range (1000–1400 users), the proposed system sustains a high and stable throughput of between 715 and 720TPS, while the performance of the reference system further declines to 86TPS.

Through this comprehensive performance comparison experiment, the proposed system demonstrates significant technical advantages in both response time and throughput metrics. The performance enhancements can primarily be attributed to three innovative design features: First, the "3 + 1" multi-chain architecture, which effectively distributes business loads; second, the optimized notary mechanism, which enhances cross-chain coordination capabilities; and third, innovative strategies for cross-chain communication that boost data

interaction efficiency. The experimental results not only corroborate the rationality of the system design but also its scalability and stability in practical application scenarios, thereby providing reliable technical support for the digital transformation of port supply chains.

Security analysis

Confidentiality: The proposed system establishes a robust multi-layered security framework through layered data management and differentiated encryption strategies. It employs the SM4-ECB symmetric encryption algorithm with group keys for business information, facilitating group-based access control. This approach ensures that only authorized members can decrypt data. For core sensitive information, the system utilizes independent SM4-ECB keys for field-level encryption, assigning different keys to each field to minimize the risk of information leakage. Additionally, a notary mechanism is responsible for identity authentication and permission control, enhancing security. The "3 + 1" multi-chain architecture further bolsters data security through physical isolation.

Integrity: The integrity of data within the proposed system is safeguarded by the immutable nature of blockchain technology, augmented by cryptographic mechanisms. All warehouse receipt data is subjected to SM3 hash calculations and recorded on the blockchain, making unauthorized modifications easily detectable through verification failures. During cross-chain transmissions, receiving parties uphold data integrity by recalculating hash values. The integration of smart contracts and blockchain consensus mechanisms acts as a deterrent against tampering and malicious attacks.

Availability: The "3 + 1" multi-chain architecture and notary mechanism of the proposed system ensure consistent service continuity and stability. This architecture provides inherent business isolation, preventing disturbances in one chain from impacting others. The cross-chain management platform utilizes batch processing and incremental synchronization strategies to maintain stable performance, even under high loads. Experimental results indicate that the system sustains a query throughput of approximately 720TPS and a transaction throughput of 250TPS, with query latency remaining below 600ms. Furthermore, smart contracts facilitate automated execution and a data synchronization protocol, reinforcing business process continuity and data consistency.

Research findings and managerial implications

Key research findings

The cross-chain warehouse receipt management system based on the notary mechanism and ShangMi cryptographic algorithms yields the following key findings:

Multi-Chain architecture performance: The proposed "3 + 1" architecture, consisting of three business chains (production, port, and sales) and one cross-chain management platform, demonstrates exceptional scalability in high-concurrency environments. Experimental results show that under a load of 1400 concurrent users, query latency remains below 600ms with a stable throughput of approximately 720TPS, whereas the reference system exhibits latency exceeding 16000ms under equivalent conditions. The physical isolation of business chains effectively addresses data silo challenges while ensuring secure information sharing.

Layered data structure and differentiated encryption strategy: The integration of a four-layer data structure with ShangMi cryptographic algorithms achieves an optimal balance between security and performance. Performance testing reveals that the SM4-ECB algorithm maintains throughput exceeding 1100KB/s even with 5 MB data volumes, while the SM2 algorithm demonstrates a 13.0% performance advantage over RSA. This stratified approach ensures protection of sensitive information while facilitating flexible data sharing.

Notary Mechanism-Based Cross-Chain communication: Experiments confirm that this mechanism maintains a 100% operation success rate even under high concurrency, validating its effectiveness in preserving cross-chain operational consistency. The Byzantine consensus protocol, requiring verification from at least two-thirds of notary nodes, establishes a reliable framework for multi-party collaboration.

Performance optimization strategies: Batch processing, incremental synchronization, and parallel processing significantly enhance system efficiency. Transaction operations maintain a stable throughput of approximately 250TPS, representing a substantial improvement over conventional single-chain systems. The DAG-based parallel execution engine and dynamic batch processing effectively mitigate communication and computation overhead in cross-chain interactions.

Managerial implications

Based on the key findings of this research, we present the following managerial implications. The multi-chain architecture and performance optimization strategies significantly reduce system latency and increase throughput, enabling real-time warehouse receipt management and substantially enhancing business processing efficiency. Furthermore, the layered data structure and differentiated SM cryptographic algorithms address a critical challenge in multi-party collaboration—balancing information sharing with data protection—through chain isolation and field-level encryption, providing flexible yet secure protection mechanisms for sensitive business information and fostering greater trust and willingness to collaborate within digital supply chain ecosystems.

Despite these significant advancements, several limitations persist in practical applications. While the notary mechanism effectively maintains cross-chain consistency, it employs a relatively static trust evaluation model that may compromise system resilience when confronted with sophisticated security threats or node failures in complex business environments. Additionally, the comprehensive technical architecture introduces considerable implementation complexity, particularly regarding cross-chain communication optimization under extreme concurrency conditions. Organizations adopting this technology must invest in specialized blockchain

expertise and establish standardized deployment protocols to achieve the performance benefits demonstrated in experimental settings.

These implications provide practical guidance for port supply chain stakeholders considering blockchain-based warehouse receipt management systems, highlighting both the transformative potential of the proposed technical approaches and the critical factors to consider during implementation.

Conclusion and future work

This paper introduces a cross-chain warehouse receipt management model utilizing a "3 + 1" multi-chain architecture, designed to tackle the challenges of efficiency, security, and data privacy in the digital transformation of port supply chains. The collaborative efforts of the production chain, port chain, sales chain, and cross-chain management platform achieve an optimal balance between data isolation and sharing. Employing a notary mechanism ensures the security and reliability of cross-chain communications. The integration of smart contracts and differentiated encryption strategies has demonstrated significant performance benefits in experimental settings, achieving high throughput and low latency in environments with high concurrency. This proves the system's applicability and reliability in managing complex supply chain scenarios.

Despite achieving these milestones, the system still has some limitations. For example, the trust mechanism for notary nodes is relatively static, lacking effective dynamic trust evaluation, which may present challenges when responding to node failures or malicious behavior. Furthermore, while the system performs well in high-concurrency environments, cross-chain performance still has room for improvement, especially when dealing with complex business scenarios. Additionally, for cross-chain systems, exploring the design or optimization of more lightweight SM cryptographic algorithms to adapt to resource-constrained environments and further enhance performance is an important direction for future research. Therefore, future research will focus on dynamic trust evaluation, cross-chain performance optimization, and the adaptation of lightweight cryptographic algorithms, aiming to build a more secure, efficient, reliable, and scalable cross-chain warehouse receipt management system.

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Received: 11 February 2025; Accepted: 21 April 2025
Published online: 24 April 2025

References

1. Paulauskas, V., Filina-Dawidowicz, L. & Paulauskas, D. Ports digitalization level evaluation. *Sensors* **21**, 6134. https://doi.org/10.3390/s21186134 (2021).
2. Clemente, D., Cabral, T., Rosa-Santos, P. & Taveira-Pinto, F. Blue seaports: the smart, sustainable and electrified ports of the future. *Smart Cities* **6**, 1560–1588. https://doi.org/10.3390/smartcities6030074 (2023).
3. Yi, Y. Effect evaluation and optimization model of logistics supply chain in coastal ports. *J. Coast Res.* **94**, 763–767 (2019).
4. Riazi, M. et al. Design, simulation and feasibility of the innovative agricultural warehouse receipt system through dynamic programming and agent-based models. *Sci. Rep.* **14**, 23182. https://doi.org/10.1038/s41598-024-74519-w (2024).
5. Mei, Z. & Dinwoodie, J. Electronic shipping documentation in China's international supply chains. *Supply Chain Manage.* **10**, 198–205. https://doi.org/10.1108/13598540510606241 (2005).
6. Li, M., Shao, S., Ye, Q., Xu, G. & Huang, G. Q. Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robot Comput. -Integr Manuf.* **65**, 101962. https://doi.org/10.1016/j.rcim.2020.101962 (2020).
7. Cândido, G., Barata, J., Colombo, A. W. & Jammes, F. SOA in reconfigurable supply chains: a research roadmap. *Eng. Appl. Artif. Intell.* **22**, 939–949. https://doi.org/10.1016/j.engappai.2008.10.005 (2009).
8. Giannakis, M., Spanaki, K. & Dubey, R. A cloud-based supply chain management system: effects on supply chain responsiveness. *J. Enterp. Inf. Manag.* **32**, 585–607. https://doi.org/10.1108/JEIM-05-2018-0106 (2019).
9. Selvakumar, G. & Jayashree, L. S. Agile supply chain management enabled by the internet of things and microservices. In *Proc. Int. Conf. Artif. Intell. Smart Grid Smart City Appl.* 449–456 (Springer, 2020). https://doi.org/10.1007/978-3-030-24051-6_54.
10. Lee, H. & Yeon, C. Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions. *Sustainability* **13**, 11057. https://doi.org/10.3390/su131911057 (2021).
11. Liu, Y., Liu, P., Jing, W. & Song, H. H. Pd2s: a privacy-preserving differentiated data sharing scheme based on blockchain and federated learning. *IEEE Internet Things J.* **10**, 22541–22555. https://doi.org/10.1109/JIOT.2023.3321992 (2023).
12. Xue, Y. & Wang, J. Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. *Secur. Commun. Netw.* **2022**, 5842371. https://doi.org/10.1155/2022/5842371 (2022).
13. Hu, X. et al. A blockchain cross-chain transaction method based on decentralized dynamic reputation value assessment. *IEEE Trans. Netw. Serv. Manag.* **21**, 5597–5612. https://doi.org/10.1109/TNSM.2024.3433414 (2024).
14. Amico, C. & Cigolini, R. Improving Port supply chain through blockchain-based bills of lading: a quantitative approach and a case study. *Marit Econ. Logist.* **26**, 74–104. https://doi.org/10.1057/s41278-023-00256-y (2024).
15. Xie, Z. & Li, Z. A blockchain multi-chain federated learning framework for enhancing security and efficiency in intelligent unmanned ports. *Electronics* **13**, 4926. https://doi.org/10.3390/electronics13244926 (2024).
16. Jamil, A., Iqbal, N., Khan, A. & Kim, T. H. A systematic review of blockchain technology for government information sharing. *Comput. Mater. Contin.* **74**, 1799–1818. https://doi.org/10.32604/cmc.2023.049856 (2023).
17. Ding, Y. et al. A scalable cross-chain access control and identity authentication scheme. *Sensors* **23**, 2000. https://doi.org/10.3390/s23042000 (2023).
18. Pillai, B., Biswas, K. & Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **35**, e23. https://doi.org/10.1017/S0269888920000314 (2020).
19. Xiong, A., Liu, G., Zhu, Q., Jing, A. & Loke, S. W. A notary group-based cross-chain mechanism. *Digit. Commun. Netw.* **8**, 159–167. https://doi.org/10.1016/j.dcan.2022.04.007 (2022).
20. Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system (2008).
21. Ou, W. et al. An overview on cross-chain: mechanism, platforms, challenges and advances. *Comput. Netw.* **218**, 109378. https://doi.org/10.1016/j.comnet.2022.109378 (2022).

22. Gao, N. et al. Modeling and analysis of Port supply chain system based on fabric blockchain. *Comput. Ind. Eng.* **172**, 108527. https://doi.org/10.1016/j.cie.2022.108527 (2022).
23. Zheng, Z. et al. An overview on smart contracts: challenges, advances and platforms. *Future Gener Comput. Syst.* **105**, 475–491. https://doi.org/10.1016/j.future.2019.12.019 (2020).
24. Vazquez Melendez, E. I., Bergey, P. & Smith, B. Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust. *Supply Chain Manag.* **29**, 706–730. https://doi.org/10.1108/SCM-06-2023-0295 (2024).
25. Charles, V., Emrouznejad, A. & Gherman, T. A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Ann. Oper. Res.* **327**, 7–47. https://doi.org/10.1007/s10479-023-05169-w (2023).
26. Lei, L., Song, L., Wan, J., Zhang, Y. & Huang, S. Improved method of blockchain cross-chain consensus algorithm based on weighted PBFT. *Comput. Intell. Neurosci* **2022**, 9031491. https://doi.org/10.1155/2022/9031491 (2022).
27. Sun, Y., Yi, L., Duan, L., Fan, Z. & Wei, W. A decentralized cross-chain service protocol based on notary schemes and hash-locking. In *Proc. IEEE Int. Conf. Serv. Comput.* 152–157 (IEEE, 2022). https://doi.org/10.1109/SCC55611.2022.00028.
28. Martinkauppi, L. B., He, Q. & Ilie, D. On the design and performance of Chinese OSCCA-approved cryptographic algorithms. In *Proc. Int. Conf. Commun.* 119–124 (IEEE, 2020). https://doi.org/10.1109/COMM48946.2020.9141997.

Acknowledgements

The authors are grateful to all the editors and anonymous reviewers for their comments and suggestions.

Author contributions

The authors confirm contribution to the paper as follows: Conceptualization, Yangbo Chen and Wei Ou; methodology, Yangbo Chen; software, Yangbo Chen, Qiuling Yue and Wenbao Han; validation, Yangbo Chen and Qiuling Yue; formal analysis, Yangbo Chen; data curation, Yangbo Chen; writing—original draft preparation, Yangbo Chen and Wei Ou; writing—review and editing, Yangbo Chen, Wei Ou, Mengxue Pang and Wenbao Han; supervision, Jianqiang Ma; project administration, Wei Ou; funding acquisition, Wei Ou and Jianqiang Ma. All authors reviewed the results and approved the final version of the manuscript.

Funding

This work was supported by the Joint Funds of National Natural Science Foundation of China (Grant No. U23A20304), the Fund of Laboratory for Advanced Computing and Intelligence Engineering (No. 2023-LYJJ-01-033), the Special Funds of Jiangsu Province Science and Technology Plan (Key R&D Program Industry Outlook and Core Technologies) (No: BE2023005-4), the Science Project of Hainan University (KYQD(ZR)-21075).

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to W.O.