ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Research on the Implementation of Data traceability Mechanism based on blockchain in cross-border e-commerce logistics Security

Qinghan Hu[1,*] *and Linyi Wang*[1]

[1] Business School, Chengdu College of University of Electronic Science and Technology of China, Chengdu, 611731, Sichuan, China

SUMMARY: *With the continuous expansion of cross-border e-commerce scale, logistics security has put forward higher requirements for verifiable data flow, tamper-resistant records and timely location of abnormal nodes. This paper constructs a blockchain-based secure data traceability mechanism for cross-border e-commerce logistics, which integrates event standardized coding, hash anchoring, smart contract verification, alliance chain collaboration and audit writeback into a unified implementation framework. The mechanism covers data access, index construction, on-chain execution, consistency audit and traceability query, and can support the trusted association between order events, warehousing records, customs status, transportation updates and receipt information. The experiment was carried out on the Fabric test platform consisting of 28 nodes and 1.26 million logistics records. The results show that the proposed method achieves 2147 TPS, 1.84 s average confirmation delay, 98.6% tracking accuracy and 96.9% abnormal node location accuracy, and maintains a relatively stable output under the conditions of high concurrency, field tampering and signature replacement. The mechanism can provide reliable data support for supply chain collaboration, supply chain financial verification and e-commerce supervision.*

KEYWORDS: *Supply chain; Supply chain finance; Electronic commerce*

1 Introduction

In the context of the continuous extension of cross-border e-commerce transaction links, logistics security is no longer just a transportation link operation requirement, but a data coordination requirement throughout the whole process of order generation, storage distribution, customs declaration verification, trunk line transportation, terminal signing and dispute backtracking. The business interface, document format, responsibility subject and timeliness rules between different countries and platforms are not consistent. Logistics records are often stored in various forms such as platform databases, enterprise business systems, Internet of things terminal logs and manual input information. The data mapping relationship is complex, the record update rhythm is not uniform, and the safety verification is difficult to maintain a consistent. In this operating environment, the construction of verifiable, traceable and auditable data flow mechanism for cross-border e-commerce logistics security has become an important part of e-commerce computing system design.

Zhou et al. conducted bibliometric analysis on blockchain-enabled cross-border e-commerce supply chain management, and summarized the technological evolution paths of cross-organizational collaboration, transparent flow and trusted sharing in international

*huqinghan0910@126.com
https://doi.org/10.65102/is2026324 Published: 30 April, 2026

e-commerce scenarios, which provided a clear reference for data governance modeling in cross-border links [1]. Ni et al. studied the supply chain traceability system based on blockchain, discussed the implementation boundaries of traceability mechanism in applicability, deployment conditions and collaborative game, and showed that the trusted ledger structure can provide a stable data alignment foundation for multi-node business environment [2]. Omar et al. proposed a blockchain traceability scheme for the supply chain of medical protective equipment, and fine-grained binding of traceability records and circulation events verified the feasibility of chain storage for cross-node material flow verification [3]. Marchese et al. designed a blockchain-based agricultural and food product traceability management system, which established a closed-loop logic between data registration, status verification and source identification, demonstrating the deployment of distributed architecture in heterogeneous supply networks [4]. Ferrandez-Pastor et al. proposed an agricultural traceability model integrating iot and blockchain, which integrates field collection, state encapsulation and on-chain confirmation into a unified process, indicating that effective coupling can be formed between sensing terminals and trusted storage [5].

El Azzaoui et al. studied the distributed information hiding framework based on blockchain, and introduced privacy preservation mechanism into medical supply chain data protection, which further expanded the security expression ability of traceability system in sensitive data processing [6]. Hader et al combined blockchain and big data technology to apply to traceability and information sharing in the textile industry, indicating that high-dimensional business records can provide higher data consistency for cross-subject logistics collaboration after structured processing [7]. Ugochukwu et al. studied the logistics management system based on the combination of blockchain and Internet of things, which built a trusted interactive link between resource scheduling and event record, and strengthened the real-time verification ability in the logistics process [8]. Ugochukwu et al. also proposed a secure logistics management architecture combined with RSA asymmetric encryption, so that transaction record, identity authentication and access control can operate in the same computing framework in coordination [9]. Ehsan et al. constructed a blockchain-driven conceptual model of agricultural product supply chain, and further explained that the synchronous design of business processes, status data and node permissions is the basis for improving traceability credibility and execution stability [10].

Existing research has provided important support for logistics traceability, data protection and distributed collaboration. However, in the security scenario of cross-border e-commerce logistics, order data, customs clearance data, trajectory data and signature data often belong to different platforms and responsibility units. It is difficult to form a close correspondence between the on-chain record and the offline state, and the system operation results are difficult to directly serve the abnormal location, responsibility identification and performance verification. Compared with the internal tracking of a single enterprise, the multi-source data in cross-border logistics not only has the requirement of time continuity, but also has the computational properties of trusted node identity, verifiable state switching and replay of evidence chain, which makes the design of traceability mechanism no longer stop at information summary, but need to be built for the consistency of distributed system, automatic contract execution and security audit capabilities as a whole.

Based on this background, this paper focuses on the requirements of trusted data flow in cross-border e-commerce logistics security, constructs a blockchain data traceability mechanism, and completes the implementation design from the aspects of data chain, hash anchor, event mapping, smart contract verification and exception backtracking. On this basis, combined with the computer system test method, the throughput capacity, confirmation delay,

traceability accuracy, abnormal node positioning effect and operation stability are verified, so that the technical value of the blockchain mechanism in the intersection scenarios of supply chain, supply chain finance and e-commerce can be quantified.

2 Literature Review

The application of blockchain in supply chain digitization has expanded from simple data storage to multiple computing levels such as access control, process collaboration, contract execution and trusted audit. For cross-border e-commerce logistics, order flow, payment flow, customs flow and transportation flow have the common characteristics of concurrent update, high-frequency interaction and cross-platform mapping. The literature review should not stay in the general supply chain scenario, but focus on the data organization on the chain, node authority management, traceability depth design and system operation efficiency. Bai et al. studied the adoption constraints of blockchain in supply chain finance and pointed out that there was a tight coupling relationship between data trusted sharing, participant collaboration and system embedding, indicating that once logistics data had verifiable attributes, financial verification and performance judgment could obtain a more stable evidence base [11]. Li et al. proposed a blockchain secure storage and access control scheme for supply chain ecological business data, and took the automobile industry as an example to show that detailed granularity authorization, on-chain index and controlled access can simultaneously improve data security and system manageability [12]. Ahmed et al studied the width and depth of supply chain traceability supported by blockchain, emphasizing that traceability design is not only the expansion of record number, but also the collaborative matching of object granularity, process level and information penetration ability. This view has direct inspiration for the event modeling of package level, batch level and order level in cross-border e-commerce logistics [13]. The Islam system sorted out the research path of blockchain to realize supply chain security, and incorporated identity authentication, consensus trust, privacy protection and risk mitigation into a unified analysis framework, indicating that security goals need to be supported by architecture design and mechanism implementation [14]. Sarfaraz et al. proposed the AccessChain access control framework, which strengthened the data protection capability in the blockchain supply chain environment through the linkage of permission rules and data access logic on the chain, and also provided a transferable idea for the authorization management of multi-role nodes in cross-border logistics [15]. Gomasta et al. constructed the PharmaChain drug supply chain source verification system, which integrated source record, status verification and verification path into the same traceability process, reflecting the structural value of verification system for anomaly identification and evidence playback [16].

In terms of automatic execution of logistics and supply chain, Alqarni et al. studied the application of logistics and supply chain based on blockchain smart contracts, and pointed out that contract rules can transform business actions such as confirmation, delivery, signature verification and responsibility triggering into executable code, thereby reducing manual dependence in cross-agent collaboration [17]. Wu et al. proposed an efficient blockchain-based supply chain traceability method, focusing on the balance between traceability response speed, on-chain processing efficiency and overall system availability, which provides a strong reference for performance design in the environment of high-frequency logistics events [18]. Azevedo et al. studied the implementation path of supply chain traceability using blockchain, and showed that transparent records on the chain and cross-party sharing mechanism can improve the visibility of flow, but the system deployment still needs to be synchronized with business process reconstruction [19]. Duan et al. summarized the application status and future

opportunities of blockchain in supply chain management, and further pointed out that data mutual trust, process standardization and platform compatibility are important conditions for the continuous implementation of the system [20]. Sharabati et al. reviewed the application of blockchain in supply chain management from the perspective of implementation, and believed that the system construction needs to consider technology maturity, organizational coordination ability and scene matching degree at the same time, which makes the blockchain scheme no longer a single software deployment, but a comprehensive project through data structure, process logic and governance interface [21]. The above studies constitute an important basis for the research of cross-border e-commerce logistics security, but the focus of different literatures is not consistent. Some prefer on-chain storage and access control, some prefer deep traceability design, some prefer smart contracts and business execution, and some prefer system implementation conditions. For comparison purposes, Table 1 summarizes representative directions in related studies.

Table 1: Comparison of related studies on blockchain supply chain traceability

References	Research Direction	Core Mechanism	Inspiration for This Study
[12]	Secure storage of supply chain business data	On-chain indexing and fine-grained access control	Provides a structural reference for multi-role data authorization in cross-border logistics
[13]	Traceability breadth and depth in supply chains	Multi-level traceability object design	Provides a basis for event modeling at the order, batch, and parcel levels
[15]	Blockchain-based access control framework	Linkage between permission rules and on-chain access	Applicable to permission verification across cross-platform nodes
[17]	Application of smart contracts in logistics	Code-based execution of business rules	Can support automated processing of signing, authenticity verification, and responsibility triggering
[18]	High-efficiency blockchain traceability	Coordination of traceability response and processing efficiency	Can be used for performance optimization under high-frequency logistics events
[21]	Review of blockchain implementation	Coordination of technology, organization, and application scenarios	Supports analysis of system implementation and deployment conditions

It can be seen from the existing results that the research on blockchain traceability has shifted from single point of record to multi-layer data linkage, but the calculation requirements in cross-border e-commerce logistics security still have stronger complexity. First, the data sources of cross-border logistics are complex, and warehousing scanning, customs clearance receipt, transportation trajectory, signature and dispute proof are distributed in different systems. Without unified event coding and hash anchoring mechanism, it is difficult to maintain a stable mapping between on-chain records and business states. Secondly, logistics security depends not only on certificate storage, but also on rights control, status verification and anomaly location. Therefore, the access control framework, smart contract rules and traceability query mechanism need to be deployed in the same system. Third, the

cross-border e-commerce scene has obvious characteristics of high concurrency, and the package event updates are intensive. The system must take into account writing efficiency, confirmation delay and operation stability. Based on this, on the basis of existing research, this paper brings data uplink rules, contract trigger logic, traceability path reconstruction and abnormal node identification into a unified implementation framework, and takes operational performance, security verification and positioning effect as the focus of subsequent evaluation, so that the research object and cross-border e-commerce logistics security scenarios maintain strict correspondence.

Compared with general supply chain traceability, the research scenario corresponding to this paper places more emphasis on cross-platform exchange, cross-subject verification, and cross-link evidence closure. Secure storage, rights management, source verification, and smart contract execution in the literature provide a method reserve for the trusted flow of cross-border logistics data. However, for the playback of abnormal events, responsible node positioning, and the consistency of on-chain and off-chain states in logistics security, closer computational integration is still needed. Therefore, the purpose of the literature review is not only to show that blockchain can be used for traceability, but also to clarify which mechanisms can directly serve the security implementation of cross-border e-commerce logistics, and which structures can support subsequent system testing and effect analysis.

3 Methods and materials

3.1 Design of data uplink and data traceability mechanism for cross-border e-commerce logistics security

The security data in cross-border e-commerce logistics is not an isolated record generated by a single node, but the result of multiple events continuously transmitted between different platforms, such as order generation, storage allocation, entry and exit declaration, trunk line handover, terminal receipt and dispute proof. In order to make the blockchain truly assume the traceability function, the objects written on the chain can not only be simple copies of the original form, but also need to complete event extraction, field compression, identity binding, summary calculation and path index construction, so that the data on the chain can not only correspond to the real business, but also support subsequent query, verification and exception replay. Based on this idea, this paper divides cross-border logistics data linking into six continuous links: event normalization, summary anchoring, trusted filtering, link splicing, root value verification and anomaly location, so that the order-level, package-level and node level information can be consistent in the same traceability framework.

In order to compress the logistics records with different sources, granularities and formats into a uniform writable object, and maintain the structural stability of the event-level traceability unit, this paper first defines the normalized mapping function of the original logistics event as follows:

$$x_i=\phi(o_i,p_i,n_i,t_i,g_i,a_i,s_i)=W_e\left[e(o_i)\|e(p_i)\|e(n_i)\|e(a_i)\right]+W_t\tau(t_i)+W_g\gamma(g_i) \tag{1}$$

where x_i represents the normalized representation vector of the i logistics event, o_i represents the order identity, p_i represents the parcel identity, n_i represents the execution node identity, t_i represents the timestamp, g_i represents the geographic section, a_i represents the operation type, s_i represents the original signature summary. $e(\cdot)$ denotes the discrete field embedding function, $\tau(\cdot)$ denotes the temporal encoding function, $\gamma(\cdot)$ denotes the geographic mapping function, and W_e, W_t, and W_g are projection matrices. The

function of this formula is not simply to do feature concatenation, but to uniformly compress business semantics, temporal location and spatial attributes into the same representation space, which provides consistent input for subsequent hash calculation and index construction.

In order to make each normalized logistics event form an irreversible summary before being put on the chain, and ensure that the index on the chain can stably point to the original source of the chain, this paper further defines the event hash anchoring function as follows:

$$h_i=H(x_i\|b_i\|r_i\|\sigma_i) \tag{2}$$

where h_i represents the event summary value, $H(\cdot)$represents the secure hash function, b_i represents the service batch number, r_i represents the node role coding, and σ_i represents the node private key signature result. This formula encodes event representation, business batch, role information and signature summary together, so that records generated by the same package at different processing nodes can form a concatenable evidence sequence, and makes it difficult for field substitution, role forgery and local tampering to bypass summary verification.

Its structural organization is shown in Fig. 1. After heterogeneous records such as order creation, warehouse scanning, customs declaration receipt, transportation update and receipt confirmation are entered into the access terminal, the system first completes field standardization, time alignment and node identity mapping, and then divides them into independent event units according to order number, package number and operation type. Then, the unified representation of the event unit is generated by standardized coding, and the hash summary is further calculated to form the event identity and the correlation index. After wrapping the summary, the smart contract writes the event summary, state label and index pointer to the blockchain ledger, while keeping the original details in the off-chain storage area. The structure formed in this way is not simply "data linking", but organizes the original record, event summary and traceability entry into a verifiable, locatable and replayable traceability basic unit, which provides direct support for subsequent link reconstruction and anomaly verification.

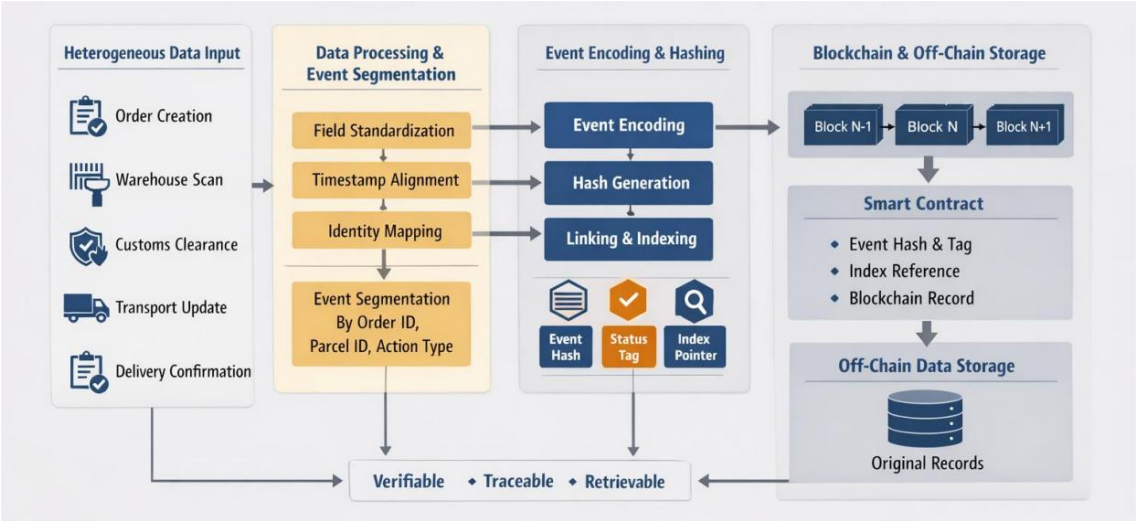

Figure 1: Flow chart of cross-border e-commerce logistics events linking and index construction

The fact that a single event is successfully written to a block does not mean that a full traceability link has been formed. The time granularity, node naming method and status field

granularity between cross-border logistics platforms are not consistent. If there is no event credibility determination and sequential correlation mechanism, it is difficult to automatically restore the record on the chain to a continuous path. To this end, after the abstract is written, this paper continues to introduce three calculation links: credibility score, association weight and soft alignment probability.

In order to simultaneously examine signature validity, time offset and field completeness at the source stage, and restrict low-trusted records from entering the traceability main chain, this paper constructs a single-event trust scoring function as follows:

$$c_i=\alpha v_i+\beta \exp\left(-\frac{|\Delta t_i|}{\eta}\right)+\gamma q_i, \quad \alpha+\beta+\gamma=1 \tag{3}$$

where c_i represents the event credibility score, v_i represents the signature truth verification result, Δt_i represents the offset between the event and the theoretical time series window, q_i represents the integrity of the state field, η represents the time attenuation coefficient, α, β, γ are weight parameters. This formula compreses three types of information, such as credible identity, reasonable timing and complete field, into the same scoring framework, so that low-quality events are weakened before they enter the main chain, and the stability of traceability results is guaranteed from the source.

In order to connect the discrete summaries generated by adjacent nodes into a replayable logistics trajectory, and maintain the continuity constraints in time and space in the multi-hop path, this paper defines the correlation weights between events as follows:

$$w_{ij}=c_i c_j \exp\left(-\frac{|t_j-t_i|}{\lambda_t}\right)\exp\left(-\frac{d(g_i,g_j)}{\lambda_g}\right)1(p_i=p_j) \tag{4}$$

Here, w_{ij} represents the association weight between event i and event j, $d(g_i,g_j)$ represents the geographic segment distance, λ_t and λ_g represent the temporal and spatial scale parameters, respectively, and $1(p_i=p_j))$ represents the parcel identification consistency indicator function. This formula simultaneously constrict temporal proximity, spatial proximity and object consistency, so that path splicing does not rely on manual alignment, and the backbone order is automatically recovered by calculation rules.

In order to complete the cross-source event alignment under the condition of multi-platform records and weaken the path bifurcation caused by repeated scanning and asynchronous backtransmission, the soft alignment probability of cross-source events is given as follows:

$$p_{ij}=\frac{\exp(\theta^{\top} z_{ij})}{\sum_{k\in N(i)}\exp(\theta^{\top} z_{ik})} \tag{5}$$

Here, p_{ij} represents the alignment probability of event i to event j, z_{ij} represents the feature vector composed of time difference, space difference, role difference and summary similarity, θ represents the parameters to be learned, and $N(i)$ represents the set of candidate alignments. This formula selects the optimal connection object among the candidate successor events through the normalized probability, which can effectively reduce the ambiguity path generated when multi-source records are sent back concurrently.

Its traceback reconstruction logic is shown in Fig. 2. Fig. 2 takes the above event summary as the starting point, and further concatenates the trust scoring module, the

association weight module and the cross-source alignment module to form a complete mechanism from single-event verification to multi-event path reconstruction. After the query request enters, the system first retrievesthe index directory corresponding to the target package, and then filters out the weak evidence events according to the credibility score, and then reconstructs the transport backbone according to the association weight and alignment probability. When there is a broken edge, a duplicate edge, or an abnormal jump, the system immediately switches to the backtracking verification process. The traceability chain thus formed is not a static display sequence, but can directly support anomaly identification and responsibility location.

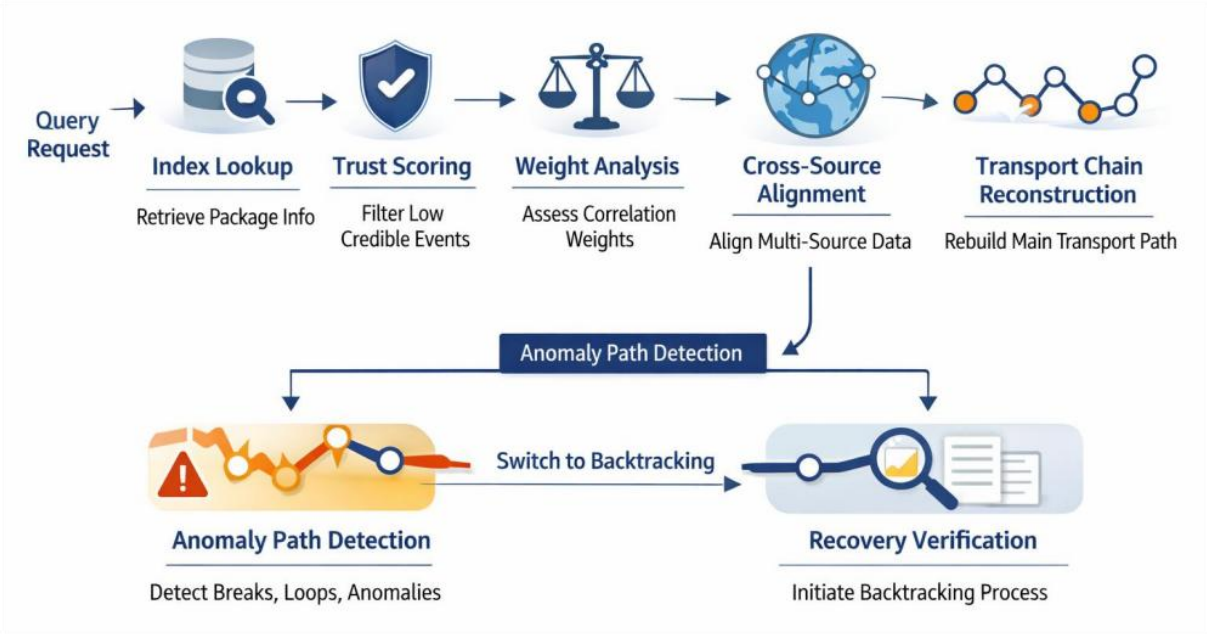

Figure 2: Mechanism diagram of cross-border logistics data traceability path reconstruction and abnormal backtracking

After the path reconstruction is completed, the system also needs to verify the whole link. Only when the constraints of key node coverage, temporal closure, summary consistency and field matching are satisfied at the same time, the traceability result has auditable value. Motivated by this consideration, this paper proceeds to define root summary aggregation, integrity measure, and anomaly localization functions.

In order to compress the multi-hop logistics path into a single verifiable root value and improve the consistency verification efficiency of the batch verification and order verification stages, this paper defines the path root summary aggregation function as follows:

$$R_{\pi}=H\left(\bigoplus_{i\in\pi}\rho_i\, h_i\right) \tag{6}$$

Here, R_{π} denotes the root digest of path π, $\oplus$ denotes the concatenation operation in order, ρ_i denotes the event position weight, and h_i denotes the hash digest of the i event. This formula compreses multi-node events into a single root value, and makes the link consistency verification transform from multiple local comparisons to a global matching, thereby reducing the computational overhead in backtracking.

In order to quantitatively measure the completion degree of a traceability path in terms of

key node coverage, temporal closure and field consistency, this paper constructs traceability integrity indicators as follows:

$$\Gamma_{\pi}=\frac{1}{|\pi|}\sum_{i\in\pi} c_i \cdot \delta_i \cdot \kappa_i \tag{7}$$

Here, Γ_{π} denotes the path integrity score,$|\pi|$ denotes the path length, c_i denotes the event credibility score, δ_i denotes the critical node coverage marker, and κ_i denotes the field consistency coefficient. The formula aggregates the local reliability inside the path into a global metric, which can screen out the pseudo-complete links with continuous surface but insufficient evidence, so that the subsequent result analysis can be based on more stable data.

In order to accurately locate the responsible nodes that cause link breakage, timing jump or summary mismatch, and enhance the interpretation ability of the abnormal playback phase, this paper defines the node anomaly localization score as follows:

$$A(n)=\sum_{i\in E(n)}\left[(1-c_i)+\omega_1(1-\kappa_i)+\omega_2\xi_i\right] \tag{8}$$

Here, A(n) represents the anomaly localization fraction of node n, E(n) represents the set of events generated by node n, κ_i represents the field consistency coefficient, ξ_i represents the path-breaking penalty between this event and previous and subsequent events, and ω_1 and ω_2 represent the regulation parameters. This formula accumulates the abnormal contribution of single event to the node level, and can directly give the priority verification object in the query phase, so as to shorten the positioning path of cross-border logistics security verification.

Through the above design, the order, package, node, status and signature information in cross-border e-commerce logistics are unified into the event-driven data traceability framework. The framework not only retains the support of blockchain for non-tampering and verifiable writing, but also extends the static ledger into a computable, comparable and replayable traceability system through normalized mapping, trust scoring, path reconstruction, root value verification and exception location, which provides a direct basis for the smart contract scheduling, interface coordination and secure execution process in the next section.

3.2 Implementation architecture of cross-border logistics security based on blockchain and smart contract

The key to the security implementation architecture of cross-border e-commerce logistics is not to simply add nodes on the chain, but to make order events, logistics status, authority control and contract execution form a stable closed loop in the same distributed environment. Therefore, on the basis of the above data chain and traceability modeling, this paper further constructs a cross-border logistics security implementation architecture based on blockchain and smart contract. The architecture adopts the deployment method of alliance chain, which integrates the logistics platform, warehousing node, customs interface, transportation node and supervision terminal into the unified ledger network, and logically divides the execution on the chain into access layer, index layer, contract layer, execution layer, audit layer and service layer.

In order to make multi-source logistics requests complete unified identity resolution and business mapping before entering the consortium chain, and ensure that cross-organizational messages enter the same execution channel, this paper defines the structured encapsulation

function of access requests as follows:

$$M_i=\langle id_i, pkg_i, role_i, act_i, ts_i, ch_i, sig_i\rangle \tag{9}$$

Here, M_i represents the standard message object of the i access request, id_i represents the business subject identity, pkg_i represents the parcel or order entity identity, $role_i$ represents the node role, act_i represents the service action type, ts_i represents the timestamp, ch_i represents the target service channel, and sig_i represents the original signature. The function of this formula is to encapsulate the records from different sources such as storage, transportation, customs and receipt into executable messages, so that the subsequent indexing and contract scheduling no longer rely on the private format of the platform.

In order to generate verifiable permission tokens synchronously in the node access stage and limit the writing scope of unauthorized roles to sensitive logistics status, this paper further defines the role token generation function as follows:

$$\Psi_i=H\left(id_i\|role_i\|scope_i\|exp_i\|nonce_i\right) \tag{10}$$

Here, Ψ_i represents the node token digest, $scope_i$ represents the allowed data domain, exp_i represents the session expiration time, $nonce_i$i represents the one-time random number, and $H(\cdot)$ represents the hash function. The identity, role, scope and time are bound to the same token, so that the manufacturer, the warehouse, the carrier, the customs clearance service provider and the regulatory end share a set of ledgers, but maintain a clear authority boundary, so as to move the access control to the transaction entry stage.

Its operating structure is shown in Fig. 3. Fig. 3 mainly shows the execution link of the cross-border logistics security architecture from the external request into the ledger confirmation return. Multi-source service requests are first verified and encapsulated by the access gateway, and then distributed to the index management module to generate event index and target channel identifier. Then, the contract scheduler selects the corresponding contract template according to the business action, and the execution node completes the writing verification, status update and signature confirmation under the rule constraints. Finally, the audit module retrieves the execution summary and returns the results to the query side.

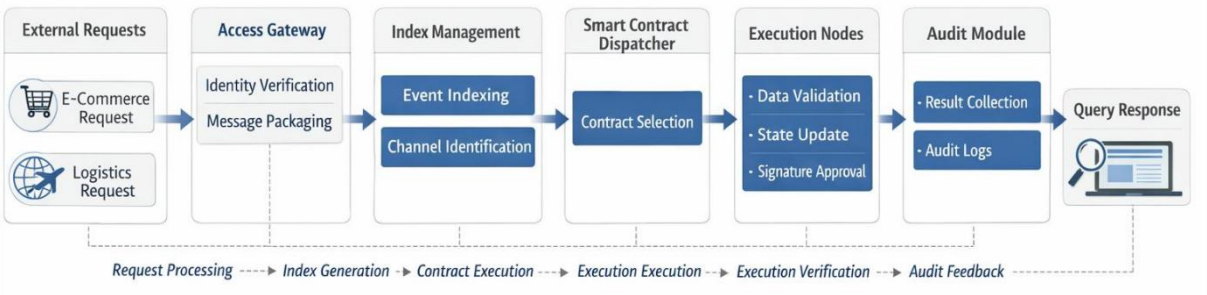

Figure 3: Flow chart of cross-border logistics security request access and on-chain execution

In the on-chain execution phase, the system does not directly regard all requests as same-weight transactions, but first jointly checks the event integrity, signature reliability and role matching. In order to describe the execution effectiveness of a single logistics event before writing, this paper gives the transaction verification score function as follows:

$$\Theta_j=\alpha s_j+\beta q_j+\gamma r_j+\delta e^{-|\Delta t_j|/\tau},\quad \alpha+\beta+\gamma+\delta=1 \tag{11}$$

Here, Θ_j represents the comprehensive verification score of the j transaction, s_j represents the signature validity, q_j represents the field completeness rate, r_j represents the role matching coefficient, Δt_j represents the magnitude of the event deviation from the standard time window, and τ represents the time decay parameter. This formula compresses the three factors of identity, field and timing into a single comparable score, so that low quality records are weakened before entering the execution pool.

In order to map different business actions to executable contracts, and automatically trigger the corresponding verification logic and responsibility record when the state changes, this paper constructs the contract trigger judgment function as follows:

$$\chi_j=\begin{cases}1, & \Theta_j\geq\theta \wedge \text{map}(act_j)=C_k\\ 0, & \text{otherwise}\end{cases} \tag{12}$$

where χ_j represents whether a transaction triggers contract execution, θ represents the transaction admission threshold, $\text{map}(act_j)$ represents the function that maps business actions to the contract template, C_k represents the k smart contract. This formula shows that the contract layer does not directly participate in consensus sorting, but acts as the core of rule execution, calling corresponding templates for actions such as warehousing, outbound, transshipment, customs declaration, signing and abnormal appeal, so that the embedded code form of business rules and the state of the ledger are promoted synchronously.

Its hierarchical organization is shown in Fig. 4. The bottom layer is the off-chain data and index support unit, which is responsible for saving the original logistics details, index mapping table and interface cache results. The middle part is the core processing area on the chain, including the index analysis layer, the smart contract layer and the execution confirmation layer, which are responsible for record positioning, permission and status rule execution, transaction verification and ledger synchronization respectively. The upper layer is the audit layer and the service output layer, which is responsible for consistency verification, exception traceback, and query display for the enterprise end, the supervisor end and the user end. The architecture organizes off-chain support, on-chain execution and result service as a continuous linkage vertical system.

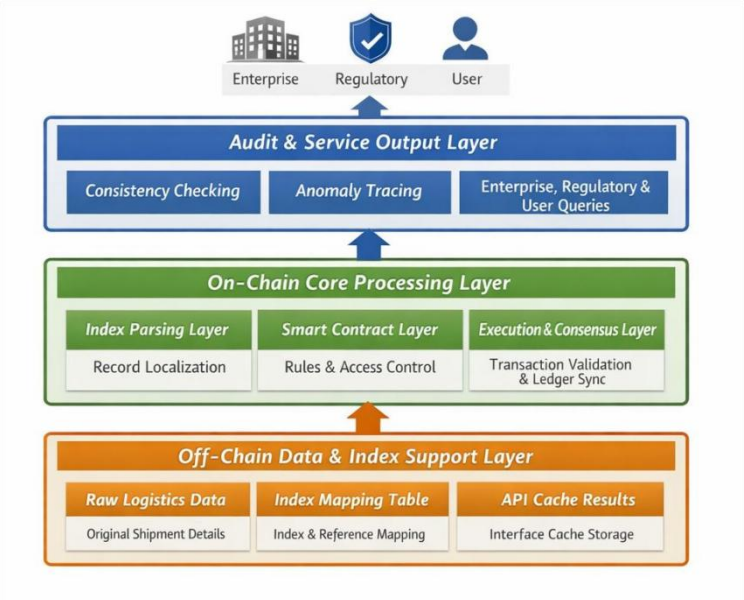

Figure 4: Hierarchical architecture diagram of cross-border logistics security alliance chain

After completing the contract execution, the system needs to further determine whether the block writing delay is still in an acceptable range. In order to describe the overall waiting cost from request entry, verification ordering, contract execution to ledger confirmation, this paper defines the block commit latency model as follows:

$$D_b=\frac{\lambda_q}{\mu(\mu-\lambda_q)}+\frac{1}{\mu_v}+\frac{1}{\mu_c} \tag{13}$$

where D_b represents the average block submission delay, λ_q represents the transaction arrival rate, μ represents the overall channel processing capacity, μ_v represents the verification processing rate, and μ_c represents the contract execution and confirmation rate. This formula not only describes the computation time of a single node, but also reflects the overall cost of request entry, verification ordering, contract execution and ledger confirmation. Therefore, it can be used to adjust the packaging threshold and concurrency window in peak hours.

In order to ensure that the on-chain results are strictly consistent with the off-chain original texts in the audit stage, and to enable the supervisor to quickly identify summary mismatch and state conflict, this paper defines the execution consistency audit function as follows:

$$A_j=\omega_1\,\mathrm{sim}(h_j,\widehat{h_j})+\omega_2\,1(y_j=\widehat{y_j})+\omega_3\,g_j,\quad \omega_1+\omega_2+\omega_3=1 \tag{14}$$

where A_j represents audit consistency score, h_j represents on-chain summary, $\widehat{h_j}$ hj represents off-chain original re-calculated summary, y_j and $\widehat{y_j}$ represent on-chain state label and off-chain state label respectively, g_j represents responsible node signature verifiability, $\mathrm{sim}(\cdot)$ represents similarity function. This formula brings hash consistency, state consistency and signature consistency into the unified audit framework. When the score is below the threshold, the system sends the record into the anomaly tracking channel.

In order to keep the transaction load in different business channels relatively balanced and reduce the impact of local congestion on the speed of ledger confirmation, this paper gives the channel routing assignment function as follows:

$$\rho_{u\to c}=\frac{\exp(w^{\top}f_{u,c})}{\sum_{m\in C}\exp(w^{\top}f_{u,m})} \tag{15}$$

Here, $\rho_{u\to c}$ represents the probability that request u is assigned to channel c, $f_{u,c}$ represents the feature vector composed of request load, channel congestion degree, action type and historical success rate, w represents the weight parameter, and C represents the set of available channels. The function of this formula is to make high-frequency logistics events automatically enter a more appropriate execution channel according to the current network status, so as to maintain the balance of the processing capacity of the alliance chain.

Its overall deployment is shown in Fig. 5. The business access terminal includes e-commerce platform, storage node, transportation node and customs interface, which is responsible for logistics events such as order generation, sorting, transshipment, declaration and receipt. The consortium blockchain coordination area in the middle is composed of blockchain nodes, smart contract engines, index services and audit services, which is responsible for transaction reception, permission verification, contract execution, block confirmation and summary verification. The result user terminal includes enterprise

management terminal, regulatory query terminal and user traceability terminal, and obtains status records and security verification results through open interfaces, forming a closed loop of "event uploading - on-chain confirmation - audit return - multi-terminal query".

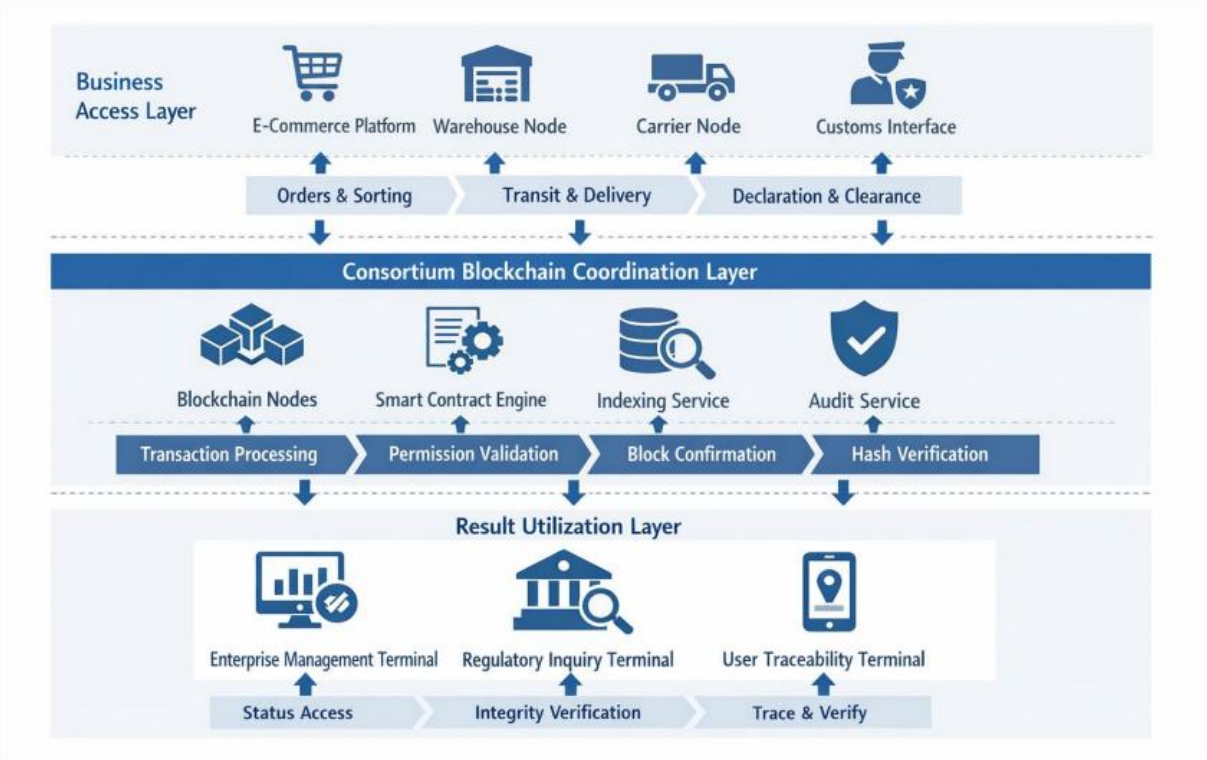

Figure 5: Overall deployment diagram of cross-border e-commerce logistics security system

In order to quantify the response quality to traceability requests in the query return phase, and to reconcile the relationship between query depth, node hit rate, and anomaly hint strength, this paper finally defines the traceability response utility function as follows:

$$U_q=\eta_1 C_q+\eta_2 L_q^{-1}+\eta_3 P_q-\eta_4 E_q, \quad \eta_1+\eta_2+\eta_3+\eta_4=1 \tag{16}$$

Here, U_q represents the overall utility of a single traceability query,C_q represents the event chain integrity rate, L_q represents the query delay, P_q represents the node hit accuracy, E_q represents the intensity of abnormal suggestion false alarm, and η_1 to η_4 are the adjustment parameters. This formula puts query quality, response speed and exception warning effect into a unified evaluation space, which can be directly used as a basis for comparing different deployment configurations in subsequent experiments.

Through the above implementation architecture, the cross-border e-commerce logistics security system completes the full-link organization from message access, permission verification, contract execution, account confirmation to audit receipt and traceability service output. The role of blockchain here is not only to keep records, but to integrate the status update, responsibility mapping and verification logic in multi-agent collaboration into an executable, queryable and reviewable computing environment, which also lays a foundation for subsequent performance testing and anomaly location analysis.

4 Results

4.1 Operational Performance and Security Verification of blockchain traceability Mechanism

In order to verify the operational performance and security stability of the constructed blockchain traceability mechanism in cross-border e-commerce logistics security scenarios, the experiment was deployed on 28 alliance chain nodes, including 20 accounting nodes, 4 audit nodes and 4 query service nodes. The bottom layer adopted the Fabric framework and connected to the smart contract scheduler. The test data includes 1.26 million orders, warehousing, customs, transportation and receipt events. The comparison method selects two typical on-chain traceback schemes, Trace-Chain and LogiBlock, and uniformizes the concurrent load, signature method and index length to ensure that the results are comparable. The test indicators cover transaction throughput, block confirmation delay, resource occupancy, summary consistency and security audit response speed.

In order to observe the change of system throughput under different concurrency intensity, Fig. 6 shows the thermal distribution of throughput under the joint effect of node size and request rate. The results show that when the request rate increases from 400 requests per second to 2200 requests per second, the throughput of the proposed mechanism continues to increase and reaches 2147 TPS under the condition of 24 nodes. After the threshold is exceeded, queuing backlogs appear in local channels, but the overall decrease is controlled within 6.3%, which indicates that hierarchical indexing and contract routing maintain a good stable release ability under high concurrency conditions.

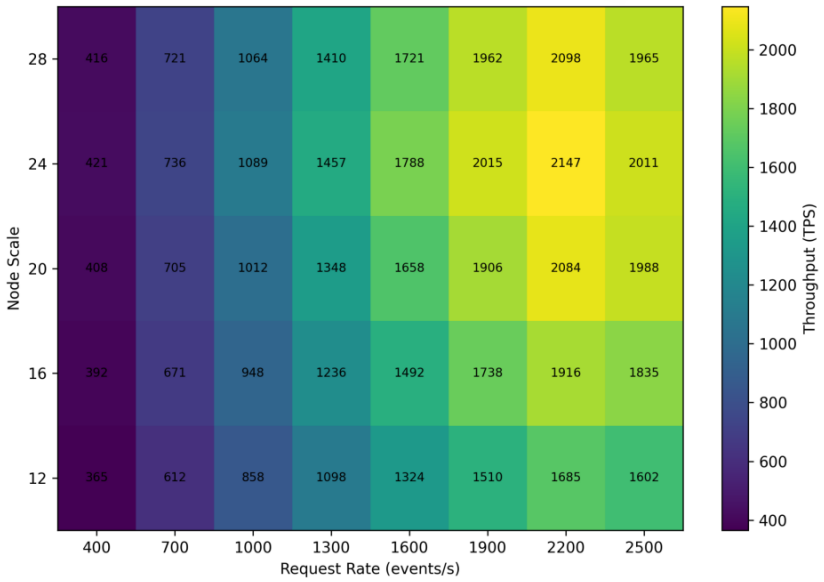

Figure 6: Throughput heatmaps for different node sizes and request rates

In order to further characterize the fluctuation characteristics of the confirmation process, Fig. 7 uses box plots to show the block confirmation delay under three conditions of normal load, peak load and mixed disturbance. The median delay of the proposed mechanism is 1.62 s under normal load and rises to 1.84 s under peak load, and the interquartile range is significantly smaller than that of the two comparison methods. Under the condition of mixed perturbation, the tail delay of the proposed mechanism stays within 2.31 s, while Trace-Chain reaches 2.94 s and LogiBlock reaches 3.08 s, which indicates that contract pre-verification

and channel routing assignment jointly compress the high bit delay.

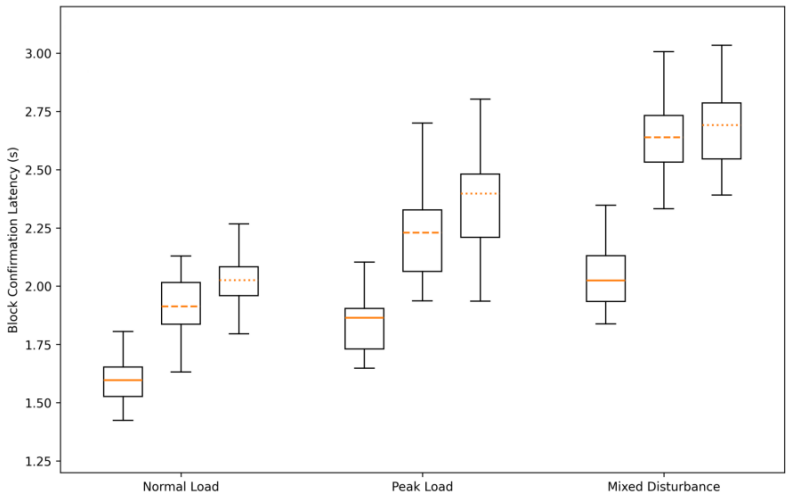

Figure 7: Boxplots of block confirmation delay under different load conditions

Fig. 8 uses a radar chart for a joint presentation of CPU usage, memory usage, disk write amplification, message retransmission rate, and audit response time. The comprehensive area of the proposed mechanism is the smallest in five indicators, in which the CPU occupation rate is 61.4%, the memory occupation is 4.8GB, and the message retransmission rate is 1.7%, which are lower than those of the comparison methods. This shows that the on-chain summary lightweight writing and off-chain original text retention strategies effectively reduce the extra consumption caused by redundant replication and repeated verification.

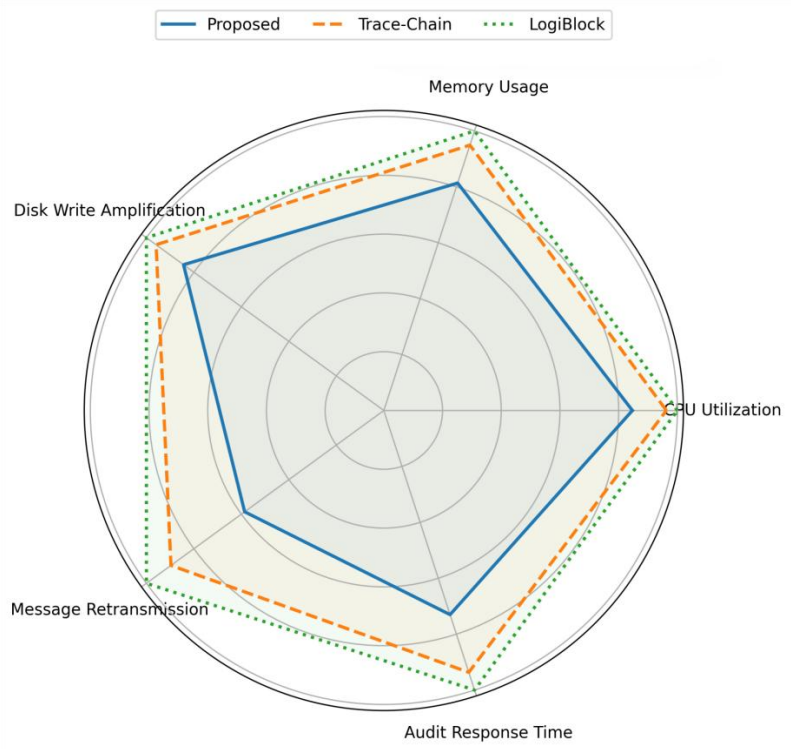

Figure 8: Integrated radar chart of running resources versus audit overhead

Fig. 9 illustrates the audit consistency matrix of different business links under normal writing, field tampering and signature replacement conditions. Under normal conditions, the consistency scores of three types of key events, including warehouse scanning, customs receipt and terminal receipt, are all higher than 0.98. After field tampering, the relevant area quickly drops to 0.21-0.34, and the score distribution after signature replacement is between 0.17-0.29. The abnormal boundary is clear and identifiable, which indicates that the mechanism can stably identify the inconsistent state of the on-chain and off-chain.

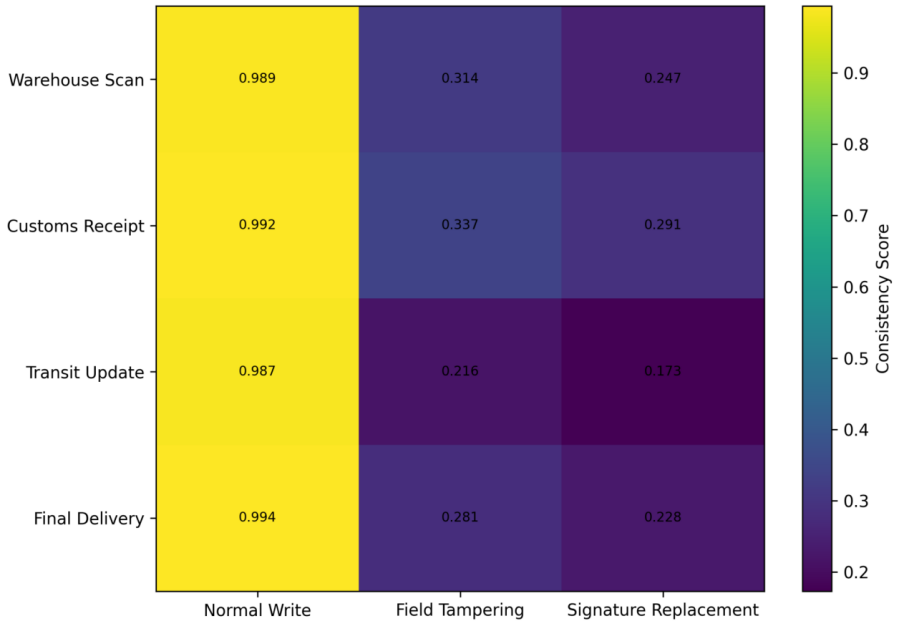

Figure 9: Event audit consistency matrix under different security conditions

In addition to graphical results, security verification requires quantitative comparisons in discrete scenarios. Table 2 summarizes the interception rate, false alarm rate, and recovery time of the three types of mechanisms under four typical attack scenarios. It can be seen that under the conditions of replay attack, unauthorized writing, index pollution and hash digest forgery, the average interception rate of the proposed mechanism is 97.8%, the false alarm rate is controlled at 2.6%, and the average recovery time is 4.7 s, which is better than the two groups of comparison methods.

Table 2: Comparison of security verification results under typical attack scenarios

Attack Scenario	Metric	Proposed Mechanism	Trace-Chain	LogiBlock
Replay Attack	Interception Rate / %	98.4	93.1	91.7
Replay Attack	False Positive Rate / %	2.3	4.8	5.1
Replay Attack	Recovery Time / s	4.2	6.7	7.1
Unauthorized Write	Interception Rate / %	97.6	92.4	90.9
Unauthorized Write	False Positive Rate / %	2.8	5.0	5.4
Unauthorized Write	Recovery Time / s	4.5	6.9	7.3
Index Pollution	Interception Rate / %	97.1	91.8	89.6
Index Pollution	False Positive Rate / %	2.7	4.9	5.6
Index Pollution	Recovery Time / s	4.9	7.2	7.8
Hash Digest Forgery	Interception Rate / %	98.1	93.0	91.2
Hash Digest Forgery	False Positive Rate / %	2.5	4.7	5.3
Hash Digest Forgery	Recovery Time / s	5.2	7.0	7.5

This result is mutual proof with the above heat map, box plot and consistency matrix, which shows that the proposed architecture not only has high throughput and low latency, but also can maintain stable output in security audit and exception recovery, which provides a reliable operation basis for subsequent traceability accuracy and node location analysis. The variance of the results of ten rounds of repeated experiments is controlled within ±3.2%, where the standard deviation of throughput is 41 TPS and the standard deviation of delay is 0.09 s, which shows that the mechanism still maintains good repeatability and engineering deployment stability under the condition of continuous load and disturbance. In the stable operation test lasting eight hours, the success rate of contract execution is above 99.3%, and the loss rate of audit receipt is only 0.4%, which shows that the system can still maintain reliable transaction closure ability under long-term operation conditions, and has stronger deployment resilience.

4.2 Analysis of data traceability accuracy and abnormal location effect in cross-border e-commerce logistics scenarios

This section further evaluates the traceability accuracy and anomaly localization effect of the proposed mechanism in the cross-border e-commerce logistics chain from the business scenario level. The test samples come from 1.26 million real structure simulation events, covering seven states: order creation, warehousing, outbound review, customs declaration, trunk transport, customs clearance and terminal receipt. In order to avoid the interference of performance indicators on the interpretation of results, this section only retains five indicators: traceability accuracy, node positioning accuracy, link integrity rate, anomaly recognition rate and response consistency, and compares them with two schemes: Trace-Chain and LogiBlock. All results are from the mean of ten independent rounds of testing with variance controlled within ±3.0%.

In order to intuitively present the traceability judgment effect of different logistics links, Fig. 10 shows the recognition confusion matrix of seven types of states on the test set. The main diagonal area of the matrix maintains high brightness, indicating that the system can stably distinguish the adjacent states such as storage, transfer, customs and receipt. Among them, there was a small amount of cross between warehousing and outbound review, but the proportion of misjudgment did not exceed 2.4%. The boundary between customs declaration and customs clearance release is the clearest, with the accuracy of 98.8% and 99.1% respectively. This result shows that the event normalized coding and index reconstruction mechanism effectively compresses the cross-platform field differences, and makes the logistics status maintain high distinguibility when tracing on the chain.

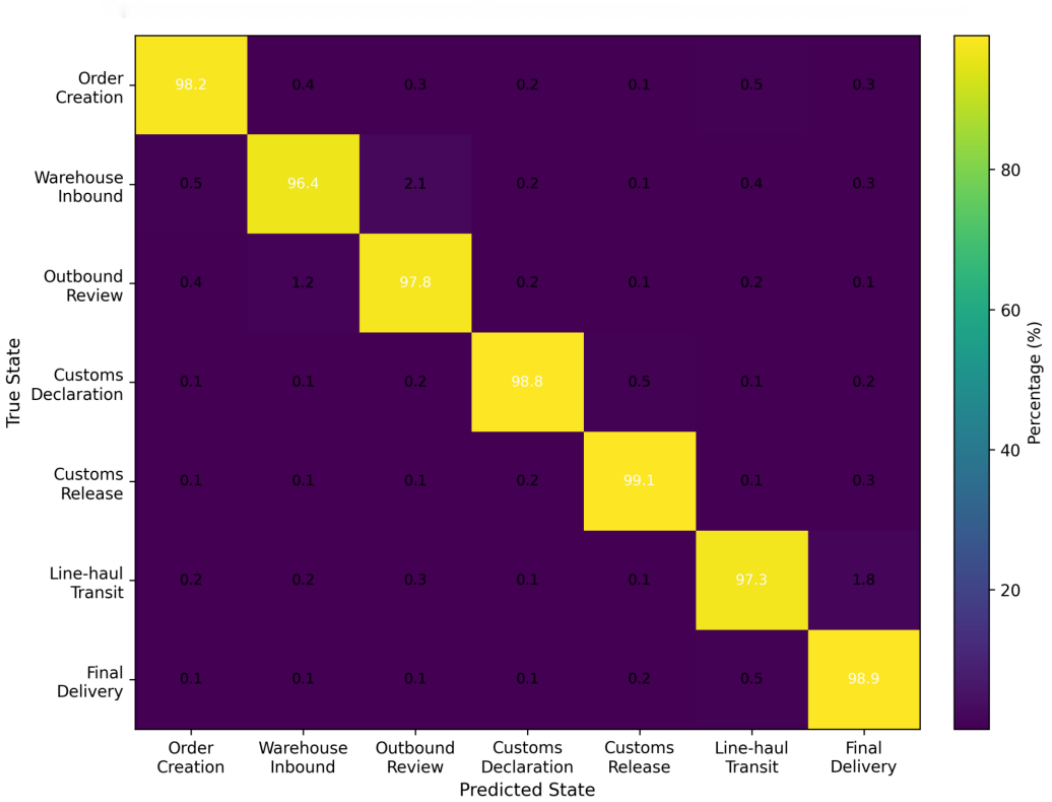

Figure 10: Confusion matrix of key status traceability results for cross-border logistics

To give an overall effect comparison, Table 3 summarizes the core results of the three mechanisms on the full test set. The traceability accuracy of the proposed method is 98.6%, the abnormal node location accuracy is 96.9%, and the link integrity rate is 97.8%, which are all higher than those of the two comparison methods. Trace-Chain maintains high recall in basic traceability tasks, but the integrity rate decreases significantly when facing cross-platform state jumps. LogiBlock is stable in link reconstruction, but it has low sensitivity to identify abnormal nodes. Combined with the performance results above, it can be seen that the proposed method does not sacrifice accuracy for throughput improvement, but forms a balanced implementation structure among index mapping, contract verification and audit writeback.

Table 3: Comparison of the overall effects of different traceability mechanisms

Method	Traceability Accuracy / %	Abnormal Node Localization Accuracy / %	Link Integrity / %	Anomaly Detection Rate / %	Response Consistency
Proposed Method	98.6	96.9	97.8	95.8	0.93
Trace-Chain	95.2	91.4	94.1	90.7	0.88
LogiBlock	96.1	92.6	95.3	91.8	0.89

In order to identify the contribution of each module to the traceability effect, Table 4 further presents the ablation experiment results. After removing the event normalization coding, the traceability accuracy drops to 94.7%, which indicates that the state mapping is easy to deviate when the heterogeneous fields are not unified. After removing the index

reconstruction module, the link integrity rate decreases most significantly, which is only 92.8%, indicating that the cross-link path recovery highly depends on the relationship between events before and after the recovery. After removing the audit writeback module, the location accuracy of abnormal nodes decreases from 96.9% to 93.5%, which indicates that the on-chain and off-chain summary comparison has a direct effect on locating responsible nodes. The complete model maintains the highest level in the three key indicators, which proves that there is a stable synergistic relationship between the modules.

Table 4: Comparison of results from model ablation experiments

Model Configuration	Traceability Accuracy / %	Link Integrity / %	Abnormal Node Localization Accuracy / %
Full Model	98.6	97.8	96.9
Without Event Normalization Encoding	94.7	95.6	93.9
Without Index Reconstruction Module	96.2	92.8	94.6
Without Audit Write-Back Module	97.1	96.4	93.5

In addition to the overall indicators, there are also differences in the identification difficulty of different business links. Table 5 presents the breakdown results for the seven categories of states. The accuracy of terminal signing, customs declaration and customs clearance is higher than 98.5%, the main reason is that these links have clear time stamps and status labels. The accuracy of mainline transshipment and warehousing review was slightly lower, but remained above 97%. The difference of anomaly recognition rate can better reflect the value of the system. Label conflict, repeated scanning and delayed return in warehousing and trunk transport are steadily recognized, and the average recognition rate reaches 95.8%. This shows that the proposed mechanism can not only recover the logistics main chain, but also return the verifiable responsibility entry in time when the state exception occurs.

Table 5: Traceability and anomaly identification results for different logistics links

Logistics Stage	Traceability Accuracy / %	Anomaly Detection Rate / %	Node Localization Accuracy / %
Order Creation	98.2	94.9	95.7
Warehouse Receiving	97.4	95.6	96.1
Outbound Verification	97.8	95.1	96.0
Customs Declaration	98.8	96.4	97.2
Line-Haul Transfer	97.3	95.8	96.5
Customs Clearance Release	99.1	96.7	97.4
Final Delivery Confirmation	98.9	96.2	97.0

On the whole, the proposed blockchain traceability mechanism shows strong ability of state recognition, link recovery and anomaly location in cross-border e-commerce logistics scenarios. For supply chain collaboration, supply chain financial verification and e-commerce platform supervision, the result output of "verifiable on the chain, replayable on the link, and locatable anomaly" is closer to the actual deployment requirements, and it also provides a reliable basis and support for the analysis of the scope and expansion space of the system in the subsequent discussion section.

5 Discussion

The blockchain data traceability mechanism constructed in this paper integrates event standardized coding, on-chain summary anchoring, smart contract verification and audit writeback into the same execution framework, so that the order flow, state flow and responsibility chain in cross-border e-commerce logistics form a verifiable and replayable closed loop. Experimental results show that the proposed mechanism achieves a peak throughput of 2147 TPS in a 28-node environment, the average confirmation delay remains at 1.84 s, the traceability accuracy reaches 98.6%, and the abnormal node location accuracy reaches 96.9%, which indicates that the service judgment ability of the system is not weakened by on-chain verification and multi-layer index. Compared with the comparison methods, the proposed mechanism still maintains high stability under the conditions of high concurrent requests, field tampering, signature replacement and index pollution, which indicates that contract pre-verification, channel routing and on-chain and off-chain consistency audit form strong coordination. From the implementation level, the advantages of the system are mainly reflected in three aspects: index reconstruction, audit writeback and consortium chain collaboration. The event-level index reconstruction improves the splicing ability of cross-platform logistics records, and makes the link integrity rate stable at 97.8%. The audit writeback mechanism directly feeds back the summary verification results to the traceability main chain, which shorts the exception location path. The deployment method of consortium blockchain reduces invalid broadcast, controls CPU occupancy and message retransmission rate. At the same time, there are still differences in interface standards, regulatory rules and data granularity in cross-border logistics scenarios, and the channel scheduling and cross-regional contract adaptation of the system under larger scale nodes still need to be enhanced. Future research can introduce partition execution, cross-chain proof, and lightweight privacy calculation to maintain higher consistency and deployment flexibility of traceability results in supply chain collaboration, supply chain financial verification, and e-commerce supervision

6 Conclusions

Focusing on the requirements of trusted data flow and traceability verification in cross-border e-commerce logistics security, this paper constructs a blockchain-based data traceability mechanism, and completes the implementation of alliance chain deployment, smart contract scheduling, event index reconstruction and audit writeback. Experimental results show that the peak throughput of the proposed mechanism is 2147 TPS under the condition of 28 nodes, the average confirmation delay is 1.84 s, the traceability accuracy reaches 98.6%, and the abnormal node location accuracy reaches 96.9%, which indicates that the on-chain summary anchoring and off-chain original text mapping can maintain the operating efficiency while supporting accurate traceability. Further analysis shows that event normalization coding enhances the alignment ability of heterogeneous data, index reconstruction improves the integrity of link recovery, audit writeback shortens the abnormal location path, and the system maintains stable output under the conditions of high concurrency, field tampering and signature replacement. The mechanism can not only provide unified computing basis for logistics status verification, responsibility mapping and security audit, but also provide trusted data support for supply chain collaboration, supply chain finance verification and e-commerce supervision. There are still some limitations in this paper. Although the test environment covers multiple types of logistics events and multiple rounds of disturbance conditions, the node scale is still mainly medium alliance chain network and has not been extended to larger

cross-regional deployment. At present, privacy protection mainly relies on permission control and summary verification, and the support for fine-grained secure computation of confidential fields is still weak. The protocol differences between customs interfaces and enterprise systems in different countries will also affect the direct migration of contract templates. In the future, cross-chain mutual recognition, lightweight privacy computing, adaptive channel scheduling and multi-region contract orchestration can be further promoted, and the continuous stability and engineering deployment flexibility of the system in complex environments can be verified by combining with larger scale real business traffic.

References

[1] Zhou F, Liu Y. Blockchain-enabled cross-border e-commerce supply chain management: A bibliometric systematic review[J]. Sustainability, 2022, 14(23): 15918.

[2] Ni S, Bai X, Liang Y, et al. Blockchain-based traceability system for supply chain: potentials, gaps, applicability and adoption game[J]. Enterprise Information Systems, 2022, 16(12): 2086021.

[3] Omar I A, Debe M, Jayaraman R, et al. Blockchain-based supply chain traceability for COVID-19 personal protective equipment[J]. Computers & industrial engineering, 2022, 167: 107995.

[4] Marchese A, Tomarchio O. A blockchain-based system for agri-food supply chain traceability management[J]. SN Computer Science, 2022, 3(4): 279.

[5] Ferrández-Pastor F J, Mora-Pascual J, Díaz-Lajara D. Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production[J]. Journal of Industrial Information Integration, 2022, 29: 100381.

[6] El Azzaoui A, Chen H, Kim S H, et al. Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems[J]. Sensors, 2022, 22(4): 1371.

[7] Hader M, Tchoffa D, El Mhamedi A, et al. Applying integrated Blockchain and Big Data technologies to improve supply chain traceability and information sharing in the textile sector[J]. Journal of Industrial Information Integration, 2022, 28: 100345.

[8] Ugochukwu N A, Goyal S B, Arumugam S. Blockchain-based IoT-enabled system for secure and efficient logistics management in the era of IR 4.0[J]. Journal of Nanomaterials, 2022, 2022(1): 7295395.

[9] Ugochukwu N A, Goyal S B, Rajawat A S, et al. An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method[J]. Mathematics, 2022, 10(24): 4670.

[10] Ehsan I, Irfan Khalid M, Ricci L, et al. A Conceptual Model for Blockchain-Based Agriculture Food Supply Chain System[J]. Scientific Programming, 2022, 2022(1): 7358354.

[11] Bai Y, Liu Y, Yeo W M. Supply chain finance: What are the challenges in the adoption

of blockchain technology?[J]. Journal of Digital Economy, 2022, 1(3): 153-165.

[12] Li S, Zhou T, Yang H, et al. Blockchain-based secure storage and access control scheme for supply chain ecological business data: a case study of the automotive industry[J]. Sensors, 2023, 23(16): 7036.

[13] Ahmed W A H, MacCarthy B L. Blockchain-enabled supply chain traceability–How wide? How deep?[J]. International Journal of Production Economics, 2023, 263: 108963.

[14] Islam M D. A survey on the use of blockchains to achieve supply chain security[J]. Information Systems, 2023, 117: 102232.

[15] Sarfaraz A, Chakrabortty R K, Essam D L. AccessChain: An access control framework to protect data access in blockchain enabled supply chain[J]. Future Generation Computer Systems, 2023, 148: 380-394.

[16] Gomasta S S, Dhali A, Tahlil T, et al. PharmaChain: Blockchain-based drug supply chain provenance verification system[J]. Heliyon, 2023, 9(7).

[17] Alqarni M A, Alkatheiri M S, Chauhdary S H, et al. Use of blockchain-based smart contracts in logistics and supply chains[J]. Electronics, 2023, 12(6): 1340.

[18] Wu H, Jiang S, Cao J. High-efficiency blockchain-based supply chain traceability[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(4): 3748-3758.

[19] Azevedo P, Gomes J, Romão M. Supply chain traceability using blockchain[J]. Operations Management Research, 2023, 16(3): 1359-1381.

[20] Duan K, Pang G, Lin Y. Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management[J]. Journal of Digital Economy, 2023, 2: 244-288.

[21] Sharabati A A A, Jreisat E R. Blockchain technology implementation in supply chain management: A literature review[J]. Sustainability, 2024, 16(7): 2823.