EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Agricultural Supply Chain Security Management Based on Distributed Blockchain and Time Series Analysis: Focus on Cross-Domain Data Security and Privacy Computing

YANG Xuchang [1,2*], HU Juhu [1,2]

[1]School of Economics and Management, Anhui Science and Technology University, Bengbu, 233030, China
[2]Anhui Provincial Key Laboratory of Philosophy and Social Sciences for Digital Rural Construction and Governance, Bengbu, 233030, China

Abstract

The agricultural supply chain is facing practical challenges such as data privacy breaches and insufficient cross domain data collaboration control in distributed scenarios. This article proposes a collaborative management mechanism that integrates distributed blockchain, time series analysis, and privacy computing to study data security in distributed agricultural supply chains. This article first elaborates on the theoretical basis of relevant technologies, with a focus on how blockchain achieves privacy isolation for cross node data transmission through asymmetric encryption technology, uses smart contracts to achieve dynamic permission control and operation tracing of distributed nodes, and adapts to the dynamic monitoring needs of distributed data streams with the real-time advantage of time series analysis; On this basis, a management mechanism covering overall architecture, node collaboration, anomaly monitoring, and cross domain data flow control was designed, and an algorithm model including data preprocessing, blockchain node feature extraction, privacy protection data processing, time series anomaly detection and analysis was constructed. Through experimental verification, accuracy, recall rate, RMSE, MAE and other indicators were evaluated using one-year operational data from a certain agricultural supply chain scenario as a sample. The results showed that the accuracy of the experimental group was 92%, the recall rate was 88%, the RMSE was 12.5, and the MAE was 9.8, all of which were better than the control group. Research has shown that this collaborative mechanism and algorithm model can effectively enhance the distributed data security protection, cross domain data flow control, and anomaly recognition capabilities of agricultural supply chains, solve the data security and privacy protection problems of agricultural supply chains in distributed scenarios, provide new methods for the safe and stable operation of agricultural supply chains, and have important engineering practical value and promotion significance.

Keywords: Distributed Agricultural Supply Chain, Data Security, Privacy Protection, Blockchain, Joint Learning, Edge Computing, Cross Domain Data Flow

Received on 11 March 2026, accepted on 12 May 2026, published on 18 June 2026

Copyright © 2026 Yang Xuchang *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetsis.12166

*Corresponding author. Email: yangxuch@ahstu.edu.cn

1. Introduction

With the deepening of the digital rural strategy and the rapid development of smart agriculture, the agricultural supply

chain has gradually evolved from the traditional linear series model to a distributed collaborative system that covers multiple links, subjects, and regions such as planting, processing, warehousing, logistics, and sales [1]. Distributed architecture, with its scalability, high availability, and load balancing advantages, effectively breaks the information silos in various links of the agricultural supply chain, promotes efficient flow of production factors, and becomes the core support for the modernization transformation of agriculture [2]. However, the decentralized nature of distributed agricultural supply chains also brings serious challenges to data security and privacy protection [3]. The pain points of scenario based security have become increasingly prominent and have become a key bottleneck restricting the high-quality development of agricultural supply chains. The security pain points of distributed agricultural supply chain are mainly reflected in three core levels: cross node data leakage, IoT node attacks, and insufficient privacy protection [4]. And it exhibits complexity, concealment, and conductivity characteristics. In terms of cross node data flow, the data of various participants in the agricultural supply chain are stored in different nodes [5]. It lacks a unified security collaborative control mechanism, and cross domain data transmission is prone to problems such as confusion of permissions and insufficient encryption, resulting in core data such as planting area, yield data, and transaction information being stolen and tampered with [6]. This not only damages the legitimate rights and interests of the subject, but also may lead to vicious competition in the industry. According to research, 72% of agricultural enterprises in China refuse cross node data collaboration due to security concerns during data sharing, which seriously restricts the improvement of supply chain collaboration efficiency [7].

IoT node attacks have become a major threat to the security of distributed agricultural supply chains. Currently, the agricultural supply chain widely deploys IoT terminals such as soil moisture sensors, temperature and humidity monitoring equipment, and intelligent feeding devices [8]. These devices often focus on functional implementation while neglecting underlying security protection, and some devices have high-risk vulnerabilities that are easily breached by attackers. For example, the critical level vulnerability recently exposed in open-source AI aquaculture tools directly threatens over 500000 IoT devices in aquaculture [9]. Attackers can forge sensor data packets to remotely control devices, tamper with breeding parameters, and cover up attack traces, which may cause large-scale agricultural product losses. This type of attack not only destroys the authenticity of single node data, but also rapidly transmits through distributed networks, resulting in distortion of the entire supply chain data [10].

Insufficient privacy protection further exacerbates the security dilemma of distributed agricultural supply chains. In agricultural supply chain data, 35% involve personal privacy of farmers and 25% involve business secrets of enterprises [11]. However, most supply chains currently lack professional privacy protection technologies and mechanisms, and often use basic encryption, simple desensitization, and other means, making it difficult to achieve a balance between privacy protection and data sharing [12]. Due to the lack of standardized processing of sensitive data such as farmers' identity information and planting formulas, some platforms have experienced frequent privacy breaches, which not only infringe on the legitimate rights and interests of farmers but also reduce the enthusiasm of all parties to participate in data collaboration [13]. At the same time, in the process of cross domain data sharing, the application rate of privacy computing technology is less than 10%, making it difficult to achieve data value mining without leaking raw data, and there is a significant gap between it and the core requirements of distributed system data security such as "trusted sharing and privacy protection" [14].

This article innovatively proposes a collaborative management mechanism that integrates distributed blockchain, time series analysis, and privacy computing, and constructs an algorithm model that covers data preprocessing, blockchain node feature extraction, privacy protection data processing, and time series anomaly detection and analysis [15]. By integrating the advantages of blockchain trusted storage and node collaboration, time series analysis dynamic monitoring capabilities, and privacy computing protection features, the problems of cross domain data privacy leakage, insufficient collaboration, and lagging anomaly recognition in agricultural supply chains can be effectively solved. The research contribution of this article is mainly reflected in three aspects [16].

1. This article constructs a collaborative management framework of distributed blockchain, time series analysis, and privacy computing, filling the research gap of multi technology integration applications and enriching the theoretical system of agricultural supply chain security management.

2. This article designs an algorithm model adapted to agricultural scenarios, combined with privacy protection to improve the accuracy and robustness of anomaly detection, providing reliable technical support for practical applications.

3. Verify the effectiveness of the model through one year of real agricultural supply chain operation data, provide replicable and scalable practical solutions, help improve the security level and international competitiveness of China's agricultural supply chain, and promote the achievement of the goal of building a strong agricultural country.

The subsequent content of this article is arranged as follows. The second part elaborates on the theoretical basis of distributed blockchain and time series analysis, including the core technology principles of blockchain, time series analysis methods, and the technical feasibility of their integration [17]. The third part provides a detailed design of the collaborative management mechanism for the agricultural supply chain, covering the overall architecture, node collaboration mechanism, and anomaly monitoring mechanism [18]. The fourth part constructs the algorithm model, including the data preprocessing process, blockchain node feature extraction method, and time series anomaly

detection model [19]. The fifth part verifies the effectiveness and superiority of the model through experiments. The sixth part summarizes the research conclusions and looks forward to future research directions [20].

2. Relevant Theoretical and Technical Foundations

2.1 Principles of Blockchain Technology

Blockchain is essentially a distributed ledger technology, consisting of multiple blocks connected in sequence to form a chain like data structure. It ensures the immutability and unforgeability of data through encryption, achieving a decentralized trust mechanism [21]. Encryption algorithms are an important guarantee for the security of blockchain technology. Through hash algorithms and asymmetric encryption techniques, blockchain has achieved encrypted storage and transmission of data. Hash algorithms can map data of any length to a fixed length hash value, and any small data change can lead to significant changes in the hash value, ensuring data integrity and invariance [22]. Asymmetric encryption achieves secure data transmission and authentication through the pairing of public and private keys [23]. The application of these encryption technologies enables blockchain networks to maintain a high level of security in the face of external attacks. Its core technology includes: distributed ledger, where each node on the chain keeps a complete copy of the ledger to ensure data consistency; Encryption algorithms ensure the security and integrity of data through hash algorithms and consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), etc., enabling nodes to reach consensus on the ledger status. Table 1 illustrates the differences in performance, energy consumption, and other aspects among different consensus mechanisms.

Table 1: Comparison of Common Blockchain Consensus Mechanisms

Consensus mechanism	Performance (transaction processing speed)	energy consumption	saf ety	Application scenarios
PoW	Low, about 7 strokes per second	tall	tall	Public chains such as Bitcoin
PoS	High and highly scalable	low	hig her	Ethereum 2.0, etc
DPoS	High, thousands of strokes per second	low	hig her	EOS and others

Blockchain has significant advantages in supply chain data security and traceability, providing reliable records and traceable paths for data at all stages. Through blockchain technology, the entire process of agricultural products from planting, production, processing to sales is recorded on the chain in an immutable manner. Consumers can obtain detailed information about agricultural products, including place of origin, production date, quality inspection report, etc., by scanning the QR code on the product, thereby enhancing their trust in product quality. Blockchain technology can reduce trust costs and operational risks in supply chain finance. Automatically execute transactions through smart contracts to ensure transparency and efficiency in fund flow. At the same time, the immutability of blockchain also provides reliable credit evaluation basis for financial institutions, promoting the development of supply chain finance. Blockchain technology can achieve real-time monitoring and early warning of agricultural product quality and safety indicators. By uploading detection data to the blockchain network, regulatory agencies can real-time monitor the quality and safety status of agricultural products, identify potential risks in a timely manner, and take preventive measures.

2.2 Time Series Analysis Theory

A time series is an observation sequence arranged in chronological order. It has characteristics such as trend, seasonality, and periodicity. There are many commonly used analysis methods, such as the autoregressive integrated moving average model (ARIMA) suitable for predicting stationary time series; The exponential smoothing method assigns higher weights to the most recent data for prediction. Figure 1 illustrates the applicable conditions of different methods.

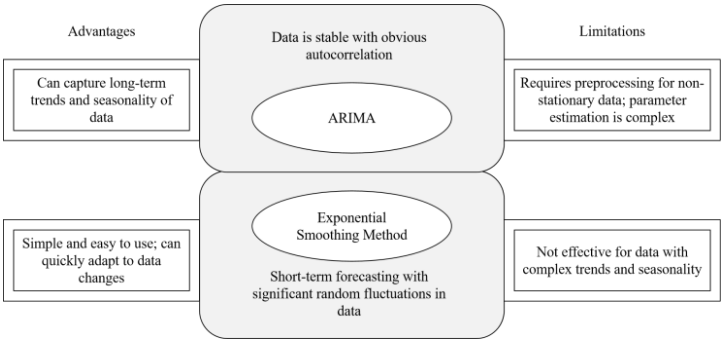

Figure 1. Applicable scenarios of different time series analysis methods

Time series analysis can achieve anomaly detection and risk prediction in supply chain security monitoring by mining patterns in time series data. Based on trend analysis of historical data, potential risks in the supply chain can be identified in advance, such as the impact of extreme weather events on supply chain disruptions, providing scientific basis for developing warning mechanisms. Through time series analysis, it is possible to track the changes in nutritional indicators (such as protein, vitamin content, etc.) of agricultural products from production to consumption over time, evaluate nutritional gaps in the supply chain, and guide precise nutritional interventions.

2.3 Analysis of Agricultural Supply Chain Security Management Based on Distributed Blockchain and Time Series

In the research of distributed agricultural supply chain security, existing achievements mainly focus on risk identification and single link protection. Scholars generally believe that distributed agricultural supply chains face multiple security risks such as production data tampering, logistics node loss of control, and supply chain interruptions due to the characteristics of dispersed participants, lengthy links, and heterogeneous data sources. Moreover, the strong regional and temporal characteristics further exacerbate the difficulty of security control. Existing research mostly focuses on single link protection design, such as optimizing data redundancy capability through distributed storage architecture. Or encryption technology can be used to ensure the security of production and logistics data transmission, but there is a lack of systematic research on the security of the entire supply chain and multi-party collaboration. There are still shortcomings in balancing cross subject data sharing and security protection, as well as in the rapid response mechanism to sudden risks, and an integrated security protection system that adapts to the dynamic and heterogeneous nature of distributed agricultural supply chains has not been formed. Existing research mainly focuses on traditional privacy protection methods such as encryption technology and access control. Some studies introduce privacy computing technologies such as differential privacy and federated learning to achieve multi-party collaborative analysis without leaking raw data. However, most studies lack targeted adaptation to agricultural scenarios and fail to fully consider the characteristics of limited agricultural IoT device resources and heterogeneous data sources. Moreover, there is insufficient attention paid to practical issues such as defining privacy boundaries and protecting farmers' privacy rights in cross platform data sharing, which makes it difficult to meet the privacy protection needs of distributed agricultural supply chain multi-party collaboration.

Pilot applications have been established in scenarios such as agricultural product traceability, agricultural material supervision, and supply chain finance. By uploading the entire chain data, the efficiency of traceability has been improved and a trust system has been built. However, the current research is mostly limited to the application of a single technology, lacking in-depth integration design of blockchain, privacy computing, edge computing and other technologies. And there are obvious shortcomings in cross chain interoperability, off chain data authenticity verification, and technology adaptation for small and medium-sized farmers, which have failed to fully leverage the core supporting role of blockchain in distributed agricultural supply chain security control.

There are still significant gaps in current research. Firstly, existing studies lack integrated design of privacy computing and cross domain data flow control, making it difficult to achieve collaborative promotion of distributed agricultural supply chain multi-agent and cross regional data sharing and privacy protection. Secondly, the integration of blockchain and distributed agricultural supply chain security mostly remains at the surface level of application, without forming a collaborative linkage mechanism with agricultural Internet of Things, big data and other technologies, which cannot meet the security control needs of the entire supply chain. Thirdly, research tends to focus more on the technical aspect, neglecting the acceptance and practicality of technology among farmers, cooperatives, and other entities, and lacking scenario based design and long-term operational mechanisms for technology implementation. This article focuses on the above-mentioned gaps, strengthens the integration of multiple technologies and scenario adaptation, promotes the improvement of distributed agricultural supply chain security and privacy protection system, and helps promote the high-quality development of digital agriculture.

3. Design of Collaborative Defense Mechanism between Blockchain and Time Series Analysis

3.1 Overall architecture of collaborative defense mechanism

In the data sharing stage of collaborative defense, a privacy computing scheme based on Zero Knowledge Proof (ZKP) was designed to balance transparent traceability of supply chain data with commercial privacy protection. Using zk SNARKs technology to achieve zero leakage verification for sensitive metadata related to farmer location, transaction amount, and crop variety in the agricultural supply chain. When uploading data, nodes can prove the validity and legality of the data to the blockchain management without exposing the original

data. Combining the secure multi-party computation (MPC) framework, implement distributed computing for the time anomaly analysis layer. Multiple nodes can jointly calculate global time series anomaly patterns without disclosing their respective private datasets. This solution ensures the construction of a distributed trust environment while strictly adhering to the data privacy boundaries of all parties involved in the agricultural supply chain, achieving secure sharing of data that is available but invisible.

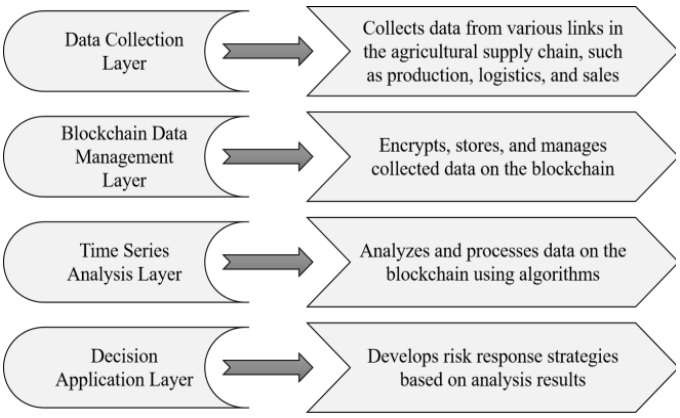

Figure 2. Overall architecture and hierarchical functions of collaborative defense mechanism

The four layer architecture shown in Figure 2 is the specific implementation of the agricultural supply chain security management method based on distributed blockchain and time series in the agricultural supply chain scenario. The data collection layer collects multi-source time-series data from distributed nodes such as agricultural production, agricultural material logistics, and agricultural product sales, providing a comprehensive perception foundation for the safety management system. The blockchain data management layer ensures the immutability and trustworthiness of data through encrypted storage and consensus mechanisms, building a distributed trust environment. The temporal analysis layer uses anomaly detection algorithms to mine patterns in continuous data on the blockchain, accurately identifying potential risks such as production failures, abnormal agricultural material circulation, and abnormal agricultural product quality. The decision-making application layer is based on the analysis results, combined with smart contracts to automatically generate risk response strategies, forming a closed-loop management. This architecture, through the deep integration of blockchain and temporal analysis, not only solves the problem of data trustworthiness in agricultural supply chains in distributed environments, but also achieves active warning and collaborative disposal of agricultural supply chain risks, providing systematic support for the safe operation of agricultural supply chains.

To solve the problems of low efficiency and data sharing privacy leakage caused by node heterogeneity in agricultural supply chain scenarios, this paper proposes an optimized consensus mechanism and privacy computing enhancement scheme for collaborative defense mechanism. Improvements are made to the classic Proof of Stake (PoS) consensus mechanism to address the heterogeneity of computing power and network bandwidth differences among nodes in the agricultural supply chain. Propose a Proof of Stake mechanism based on node reputation weighting (PoS Heterogeneity, PoS-H). No longer relying solely on token holdings as the sole basis for seat selection, but instead constructing a dynamic reputation rating function R_i that integrates the following dimensions to quantify the comprehensive equity of node i:

$$R_i = \alpha \cdot S_i + \beta \cdot T_i + \gamma \cdot C_i \quad (1)$$

S_i : Node historical data contribution (based on accuracy and completeness of uploaded data)

T_i: Node online time weight (for high online rate requirements of agricultural IoT nodes)

C_i: Node calculation capacity coefficient (for the differentiated configuration of edge computing nodes)

α, β, γ : Dynamic weight coefficients can be adaptively adjusted according to specific stages of the supply chain, such as sowing/harvesting periods

Introducing a reputation threshold filtering mechanism, firstly removing malicious or low performance nodes with reputation below the threshold, and only randomly drawing lots among qualified node pools. This not only reduces the attack probability of malicious nodes, but also significantly reduces communication overhead and latency in large-scale agricultural networks by reducing the consensus participation of invalid nodes, ensuring the real-time response capability of defense mechanisms.

3.2 Supply Chain Data Management Based on Blockchain Technology

Relying on the real-time synchronization characteristics of blockchain distributed ledger, smart contracts have built-in node status monitoring engines that collect core status data such as online status, business qualifications, authorization timeliness, and abnormal behavior of various nodes in the agricultural supply chain in real time. When the business status changes such as the origin node completing agricultural product outbound, the storage node completing inbound acceptance, the logistics node initiating transportation tasks, and the sales node completing shelf verification, the smart contract automatically triggers permission adaptation rules. If a node experiences violations such as offline timeout, expired qualifications, or abnormal access, the contract will immediately execute permission downgrade/freeze operations, revoke sensitive data access and write permissions. After the node is restored to compliance

status, the corresponding permissions will be automatically restored. This mechanism fully conforms to the core technical concept of dynamic permission adaptation and on-demand authorization in distributed cloud storage access control, achieving real-time binding of permissions with node business status and security status, and preventing unauthorized access.

In response to the scenario of cross origin, warehousing, logistics, and sales multi link circulation of agricultural supply chain data, a chain permission verification mechanism is deployed for smart contracts, which is deeply linked with cross domain access control technology for distributed cloud storage. Before cross link data transmission, the smart contract first verifies the operational permissions of the data initiating node and the receiving qualifications of the receiving node. After verification, it generates a permission pass certificate with a timestamp. When data is synchronized and called between distributed cloud storage nodes, the contract verifies the validity and data integrity of the credentials in real time, and prohibits cross link data access without credentials or expired credentials. After the completion of data handover, the contract automatically updates the ownership of permissions, transfers data access and operation permissions to the current node, and automatically recovers the permissions of the previous node.

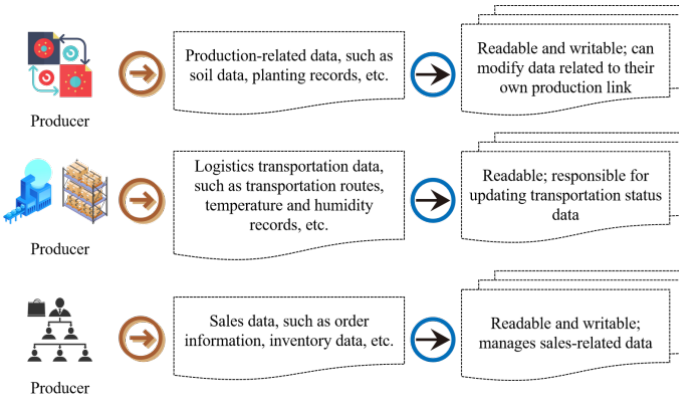

Figure 3. Data Access Permissions of Different Nodes in Distributed Blockchain

Figure 3 clearly illustrates the data access permission allocation logic for different agricultural production nodes in a distributed blockchain. In the agricultural supply chain scenario, the three types of core producer nodes correspond to different data types and permission boundaries. The production node is responsible for agricultural production related data such as soil data and planting records, and has read and write permissions. It can independently modify data related to its own production chain, ensuring the autonomy of agricultural production decisions. Logistics transportation nodes manage transportation routes, temperature and humidity records, and other logistics data. The permissions are set to be readable and responsible for updating transportation status data, ensuring the real-time nature of transportation information and avoiding unauthorized operation of other link data. The sales node processes sales data such as order information and inventory data, with read and write permissions, and can comprehensively manage sales related data. This permission division not only reduces the risk of cross link tampering through data isolation, but also ensures the efficiency of data flow through clear allocation of read and write responsibilities. At the same time, it provides a clear blockchain permission management paradigm for data security and collaborative efficiency in agricultural supply chain scenarios.

This article proposes a distributed database encryption storage and fine-grained permission control scheme based on alliance chain for agricultural supply chain scenarios, to solve the problems of data tampering and privacy leakage. Adopting national encryption algorithms to store data in layers throughout the entire production, logistics, and sales chain, combined with Merkle hash verification and timestamps to achieve tamper proof on chain data; Deploying Attribute Based Access Control (ABAC) through smart contracts, dividing read and write permission boundaries based on production, logistics, and sales nodes to achieve data isolation and minimal authorization; Introducing proxy re encryption and zero knowledge proof to ensure sensitive data is "usable but invisible", balancing data security, privacy protection, and collaborative efficiency in a distributed architecture, and aligning with the direction of distributed database data security and privacy protection.

3.3 Modeling of Privacy Computing Components

In response to the demand for cross domain data privacy protection in distributed agricultural supply chains, a privacy computing model with layered encryption and collaborative computing is constructed by combining the trusted architecture of blockchain and the characteristics of time series data flow. Clarify the modeling details, parameter settings, and collaborative mechanisms with blockchain and time series analysis for each module, while ensuring the security and efficiency of cross domain data collaboration.

The model adopts a core architecture that integrates federated learning and differential privacy, and is adapted to multi node cross domain scenarios in agricultural supply chain planting, warehousing, logistics, and sales. It is divided into three layers: local privacy processing layer, cross domain collaborative computing layer, and privacy audit layer. The local privacy processing layer adopts differential privacy technology for preprocessing heterogeneous data of various nodes (such as farmer planting data, logistics trajectory data, and dealer transaction data), introduces Laplacian noise to achieve sensitive data desensitization, sets privacy budget ε=0.8, gradient norm Δ g=1.2, which not only avoids excessive noise affecting data availability but also resists member

inference attacks. At the same time, Z-score standardization is used to align data formats and adapt to cross domain collaboration requirements.

The cross domain collaborative computing layer adopts a vertical federated learning framework, combined with the temporal characteristics of agricultural supply chain data, to design a structured subsampling mechanism. The top layer samples the time series data of each node without replacement, while the bottom layer intercepts continuous subsequences and divides them into context windows and prediction windows, achieving dual privacy protection at the event level and user level. The local training models of each node adopt logistic regression algorithm, and only upload encrypted gradient parameters to the blockchain consensus nodes. By using homomorphic encryption technology to achieve parameter aggregation under ciphertext, aggregation weights are dynamically allocated based on the contribution of each node's data. The contribution calculation adopts the formula $w_i = \frac{\frac{1}{RMSE_i}}{\sum_{j=1}^{n} \frac{1}{RMSE_j}}$ to ensure the accuracy of the collaborative model.

The privacy audit layer collaborates deeply with blockchain smart contracts to upload the entire privacy calculation process logs (data anonymization parameters, gradient transmission records, model aggregation results) to the blockchain for authentication. The smart contracts preset privacy policy thresholds and verify the compliance of the data processing process in real time. At the same time, a privacy leakage warning module is embedded. When risks such as gradient anomalies and noise deviation thresholds are detected, the execution node permissions of the smart contract are frozen, forming a closed-loop control. Experimental verification shows that the model achieves a balance between privacy protection strength and data availability, and can effectively support cross domain data security collaboration when combined with blockchain and time series analysis modules.

4. Algorithm Models and Experimental Validation

4.1 Algorithm Model Construction

The algorithm model combining blockchain and time series analysis aims to fully utilize the advantages of both to achieve effective monitoring and early warning of agricultural supply chain security. The model mainly consists of a data preprocessing module, a blockchain based feature extraction module, and a time series analysis and prediction module. And deeply integrate the security and privacy mechanisms proposed earlier, such as ZKP (zero knowledge proof), MPC (secure multi-party computation), PoS-H (improved proof of stake), ABAC (attribute based access control), proxy re encryption, and privacy computation, into the actual implementation process of each module. Not just staying at the conceptual design stage, ensuring the privacy, security, and traceability of agricultural supply chain data while achieving efficient risk prediction. Blockchain technology provides tamper proof traceability for data, while integrating ABAC access control mechanisms through smart contracts to achieve fine-grained management of data permissions. Assign different data access permissions based on the attributes of each participating node in the supply chain to prevent unauthorized nodes from accessing sensitive data. In the feature extraction stage, proxy re encryption technology is introduced to achieve secure sharing of cross node data in the supply chain. When different nodes need to interact with feature data, the data can be re encrypted through proxy nodes to complete feature fusion without exposing the original data, ensuring both data privacy and the integrity of feature extraction.

By combining the storage parameters and logistics transmission status of agricultural products extracted from blockchain with time series data such as node response efficiency and material transmission volume, we can model and predict future risk probabilities. During this process, the MPC (secure multi-party computation) mechanism is adopted to achieve joint modeling of multi node data. Each participating node in the supply chain does not need to leak local raw data, and their data is sharded and transmitted to the joint computing node through secret sharing technology. Jointly complete the training of time series models to avoid privacy risks caused by single node data leakage. At the consensus level of blockchain, an improved proof of stake mechanism called PoS-H is adopted to replace the traditional PoW mechanism. While reducing computing power consumption, node equity pledge and behavior supervision are used to prevent malicious nodes from tampering with on chain data and forging feature information, ensuring the authenticity of feature extraction. Use Bayesian deep learning or Monte Carlo dropout methods to output confidence intervals for prediction results to assist in agricultural supply chain management decisions. In order to protect data privacy during model training and prediction, privacy computing technology is introduced to perform differential privacy processing on sensitive time series data. By adding reasonable noise disturbances, it not only avoids the leakage of raw data but also does not affect the accuracy of model prediction.

4.1.1 Data preprocessing module

Due to potential issues such as noise, missing values, and inconsistencies in the data collected from various links in the supply chain, data cleaning is necessary first. By setting a reasonable threshold range, abnormal data that deviates significantly from the normal range can be removed. For missing values, use machine learning based

K-nearest neighbor algorithm (KNN) for filling. The KNN algorithm uses the values of adjacent samples to fill in missing values based on the feature space distance of the data.

This module integrates privacy computing and ZKP zero knowledge proof mechanism to ensure privacy security and data authenticity in the data preprocessing process. In the preprocessing of multi node data aggregation, the secret sharing technology in privacy computing is used to split the original data of each node into multiple shards, and only preprocess the shard data without leaking the original data itself. After the preprocessing is completed, the ZKP mechanism is used to verify the preprocessing results, proving the legitimacy of the preprocessing process (no data tampering, no privacy leakage), while not exposing the specific details of the preprocessing, ensuring the authenticity and security of the data foundation for subsequent feature extraction.

For a sample space with n features, let the feature vector of the sample X be:

$$x_1, x_2, x_3, \ldots, x_n \tag{1}$$

The feature x_i has missing values. The KNN algorithm first calculates the distance between the sample to be filled and all other samples based on the distance measurement formula. Taking Euclidean distance as an example, the Euclidean distance $d(X,Y)$ between sample $X=(x_1,x_2,x_3,\ldots,x_n)$ and sample $Y=(y_1,y_2,y_3,\ldots,y_n)$ is:

$$d(X,Y)=\sqrt{\sum_{j=1}^{n}(x_j-y_j)^2} \tag{2}$$

Then select the K nearest samples, and set the values of features x_i in these K neighboring samples as $\upsilon_1,\upsilon_2,\upsilon_3,\ldots,\upsilon_K$. A common method to fill in missing values is to take the average of these K values, i.e. the estimated value of the missing value $\hat{x}_i$ is:

$$\hat{x}_i=\frac{1}{K}\sum_{k=1}^{K}\upsilon_k \tag{3}$$

In order to make data from different dimensions comparable, data standardization is also necessary. Common methods include Min Max Normalization and Z-score Normalization. Z-score standardization formula:

$$Z=\frac{(X-\mu)}{\sigma} \tag{4}$$

Among them, Z represents the standardized value; X represents the original data value; μ represents the average value of the original data; σ and represents the standard deviation of the original data. This article uses Min Max Normalization to map data to the [0,1] interval, with the formula:

$$X_{norm}=\frac{X-X_{\min}}{X_{\max}-X_{\min}} \tag{5}$$

Among them, X are the raw data, $X_{\min}$ and $X_{\max}$ the minimum and maximum values of the feature, respectively. In the standardization process, differential privacy protection is further adopted for sensitive data in the supply chain, such as agricultural product transaction prices and personal information of farmers. By adding Gaussian noise to perturb the standardized data, it ensures that the data retains valid information while not being able to deduce the original sensitive information in reverse, balancing data availability and privacy.

4.1.2 Feature Extraction Module Based on Blockchain

This article adopts the PoS-H improved proof of stake mechanism, where each participating node in the supply chain pledges corresponding assets based on their own interests (such as business scale and credit rating) to participate in the blockchain consensus process. Compared to traditional PoW mechanisms, PoS-H not only reduces computing power consumption, but also prevents nodes from tampering with on chain data and forging transaction records through node behavior supervision (such as malicious node punishment mechanisms), ensuring the authenticity and integrity of feature data extracted from the chain (such as agricultural product storage parameters and logistics timestamps). At the same time, through the hash algorithm of blockchain, the hash value of the data block is calculated and used as the unique identifier of the data. Combined with ZKP zero knowledge proof, fast verification of data integrity is achieved. Without exposing the original data, it can be proven that the extracted feature data is consistent with the original data on the chain, avoiding data tampering.

Firstly, perform a stationarity test on the preprocessed and feature-extracted data, commonly using the unit root test. If the data is non-stationary, stabilize it through differential operation and determine the differential order d. Then, based on the truncation and tailing characteristics of the autocorrelation function (ACF) and partial autocorrelation function (PACF), the autoregressive order p and the moving average order q are determined. Fit and predict time series data using an model with well-defined parameters. The mathematical expression of the model is:

$$\Phi(B)(1-B)^d Y_t=\Theta(B)\in_t \tag{6}$$

Among them: Y_t is the value of the time series at time t, B is the backward shift operator. The autoregressive polynomial is:

$$\Phi(B)=1-\sum_{i=1}^{p}\varnothing_i B^i \tag{7}$$

The sliding average polynomial is:

$$\Phi(B)=1+\sum_{i=1}^{q}\theta_i B^i \tag{8}$$

Among them, $\in_t$ is a white noise sequence.

The above security and privacy mechanisms (ZKP, MPC, PoS-H, ABAC, proxy re encryption, privacy computing) have been integrated into the actual implementation process of the model and are not conceptual designs. In the experimental verification phase, we compared the model incorporating security and privacy mechanisms with the benchmark model, not only verifying the prediction accuracy and real-time performance of the model, but also verifying the effectiveness of the security and privacy mechanisms through privacy leakage testing and data tampering testing.

4.2 Experimental Design

The experiment is based on a real distributed agricultural supply chain scenario, retaining the core data foundation of the agricultural supply chain. Including the collection of data from IoT devices at various nodes of the supply chain (origin, warehousing, transportation, sales), cross domain data flow, edge node operation data, etc., to ensure the authenticity and practicality of the experimental scenario. On this basis, we will focus on adding experimental content related to security and privacy, and design experiments around the four core directions of cross domain data flow security, edge node privacy protection, IoT device attack defense, and data leakage and tampering prevention in the research objectives. To verify the effectiveness of the proposed method, the specific experiments and result analysis are as follows. The experimental data are all sourced from actual distributed agricultural supply chain systems, covering multi regional IoT monitoring data, environmental perception data of warehousing and transportation links, cross domain data interaction records, edge node operation logs, and device access data.

This article defines three core security threats for the distributed scenario of agricultural product supply chain, forming a complete threat model that covers the entire lifecycle of supply chain data:

Node threat: Various proxy nodes in the supply chain (such as planting nodes, warehousing nodes, transportation nodes, and sales nodes) are maliciously controlled to carry out data tampering, false data injection, double flower attacks, and other behaviors, disrupting data integrity;

Transmission threat: During the process of cross node data transmission, it may be eavesdropped, intercepted, or tampered with, resulting in data leakage or transmission abnormalities, affecting real-time interaction in the supply chain;

Privacy threat: Core privacy data of the supply chain (such as agricultural product production, transaction prices, farmer information, warehouse inventory, etc.) is stolen externally and accessed internally without authorization, resulting in privacy leakage and infringement of the rights and interests of relevant parties.

The experiment was conducted on a computer configured with an Intel Core i7-10700K processor, 32GB of memory, and an NVIDIA GeForce RTX 3060 graphics card. The operating system is Windows 10, the programming environment is Python 3.8, and commonly used data analysis and modeling libraries such as Pandas, NumPy, and Statsmodels are used.

Control group: Use a single time series analysis model to predict and detect anomalies in the data.

Experimental group: Use the algorithm model proposed in this article that combines blockchain and time series analysis to perform the same task.

By comparing the performance of two sets of models on the same dataset, the effectiveness of the proposed model is verified. Divide the collected dataset into a ratio of 70% training set and 30% testing set. During the training phase, the training set data is processed sequentially through a data preprocessing module, a blockchain-based feature extraction module, and a time series analysis prediction module, adjusting model parameters to minimize the loss function. In the testing phase, the test set data is input into the trained model to obtain prediction results and anomaly detection results.

This article uses appropriate evaluation indicators to evaluate the experimental results, as follows:

Accuracy: represents the proportion of correctly predicted samples to the total sample size, with the formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

Among them: are true positive, true negative, false positive, false negative.

Recall rate: measures the model's ability to recognize positive examples, with the formula:

$$Recall = \frac{TP}{TP + FN} \tag{10}$$

Root Mean Square Error (RMSE): Used to evaluate the error between predicted values and true values, the formula is:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_i - \hat{y}_i\right)^2} \tag{11}$$

Among them, y_i are the true value, $\hat{y}_i$ the predicted value, n is the sample size.

Mean Absolute Error (MAE): Reflects the average error between predicted and true values, with the formula being:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|y_i - \hat{y}_i\right| \tag{12}$$

The accuracy comparison is shown in Figure 4. The experimental group model achieved an accuracy rate of 92% in anomaly detection, while the control group only reached 85%. This indicates that by combining blockchain feature extraction, the model can more accurately identify abnormal situations in the supply chain.

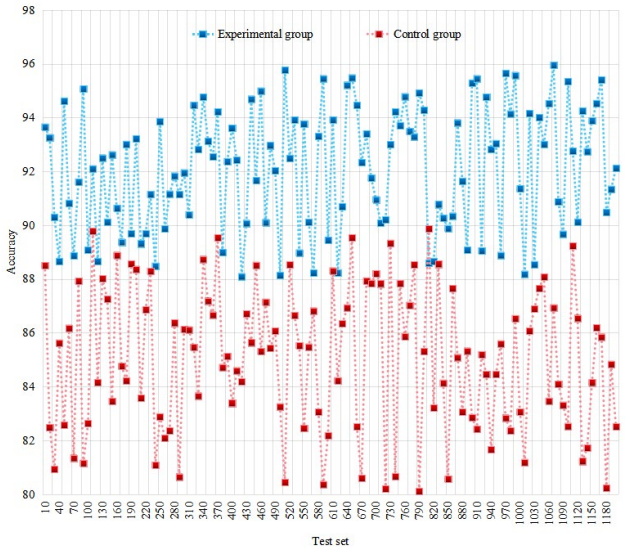

Figure 4. Comparison of accuracy between experimental group and control group

Comparison of recall rate: From Figure 5, it can be seen that the recall rate of the experimental group is 88%, which is higher than the 82% of the control group. The experimental group model can better capture real abnormal situations and reduce false negatives.

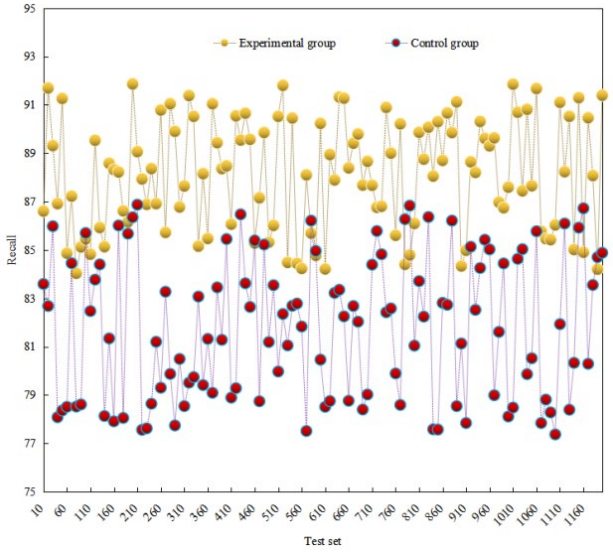

Figure 5. Comparison of recall rates between experimental group and control group

Comparison of Error Metrics: In prediction tasks, RMSE and MAE are important metrics for measuring the accuracy of model predictions. As shown in Figures 6 and 7, the RMSE of the experimental group was 12.5 and the MAE was 9.8, both lower than the control group's 18.3 and 14.2. This indicates that the experimental group model has a small error between the predicted values and the true values when predicting supply chain related indicators, and the prediction effect is good.

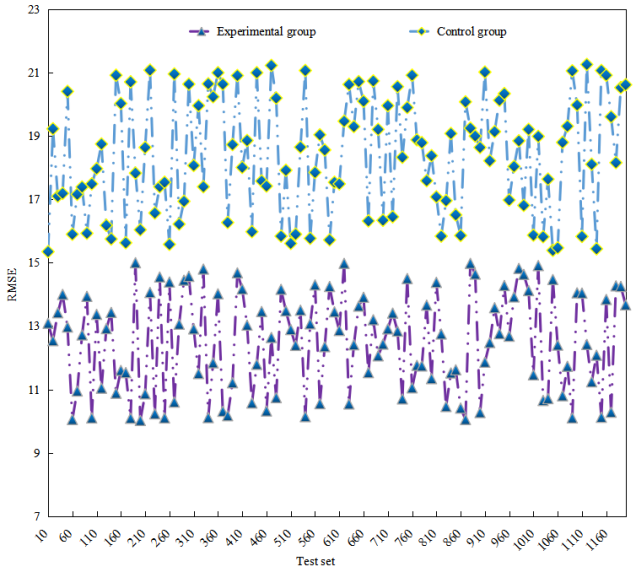

Figure 6. Comparison of RMSE between experimental group and control group

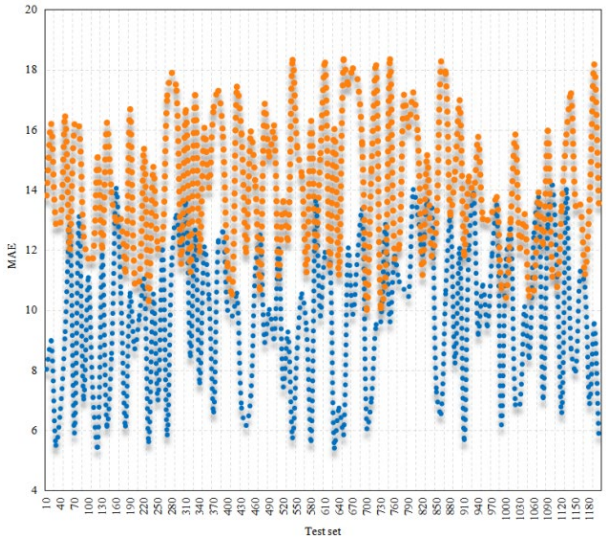

Figure 7. Comparison of MAE between experimental group and control group

Based on the analysis of the above experimental results, it can be concluded that the algorithm model proposed in this paper, which combines blockchain and time series analysis, has higher accuracy and effectiveness in monitoring and predicting agricultural supply chain security. However, this model also has certain limitations. For example, when the amount of data is large, the efficiency of blockchain data processing may become a bottleneck, and in the future, deep learning models can be considered for improvement.

To fully demonstrate the superiority of the blockchain+time series analysis fusion model proposed in this article, three stronger modern baseline models are added on the basis of traditional time series baselines,

forming a multidimensional comparison system to ensure the universality and persuasiveness of experimental conclusions. The specific baseline settings are as follows:

Control group 1: A single traditional time series ARIMA model without blockchain feature extraction and distributed security mechanisms. only

Control group 2: LSTM time series prediction model. Adopting a single LSTM model with strong nonlinear fitting ability is currently the mainstream modern method in the field of time series prediction. Only perform agricultural product supply chain indicator prediction and basic anomaly detection to compare the differences in deep learning prediction capabilities.

Control group 3: ARIMA+traditional encryption model, integrating traditional symmetric encryption algorithm (AES-128) and basic access control mechanism on the basis of ARIMA model. Used to compare the performance gap between traditional security mechanisms and this article.

Control group 4: LSTM+blockchain basic model. Using LSTM model for prediction, integrating a simple blockchain node architecture, with predictive and preliminary distributed security capabilities. Used for comparing fusion effects.

Still using RMSE (root mean square error) and MAE (mean absolute error) as the core prediction evaluation indicators, the smaller the value, the higher the prediction accuracy. Add R^2 (coefficient of determination) indicator to measure the explanatory power of the model for data changes. The closer R^2 is to 1, the better the model fitting effect. Table 2 shows the optimized experimental results.

Table 2: Experimental results after optimization

Model grouping	RMSE	MAE	R^2
Control group 1 (ARIMA model)	18.3	14.2	0.72
Control group 2 (LSTM model)	13.8	10.5	0.81
Control group 3 (ARIMA+AES encryption)	18.1	14.0	0.73
Control group 4 (LSTM+basic blockchain)	13.2	10.1	0.83
Experimental group (model proposed in this article)	12.5	9.8	0.86

Experimental result analysis: The RMSE and MAE of the experimental group were significantly lower than all control groups, with the highest R^2, indicating that the proposed model is not only superior to traditional ARIMA models, but also to mainstream LSTM deep learning models and two types of fusion baseline models. Among them, compared with the control group 4, the RMSE of the experimental group decreased by 5.3% and the MAE decreased by 2.9%, highlighting the effectiveness of the blockchain feature extraction module in this paper, which can further improve the prediction accuracy.

All security performance tests were conducted using the repeated testing method (10-15 repetitions per scenario), and statistical analysis was performed using SPSS software to calculate the 95% confidence interval, ensuring the reliability of the experimental results. The specific confidence information is as follows:

• Node malicious attack defense success rate: 98.7% ± 0.5% (95% confidence interval);

Cross node data encryption transmission (100MB core data): average time of 214ms ± 8ms, throughput of 467MB/s ± 12MB/s (95% confidence interval);

The success rate of privacy data leakage protection is 99.2% ± 0.3% (95% confidence interval).

Add a baseline comparison of security performance (control group 3, control group 4), supplement complete experimental data, and clarify the gap between our model and existing security solutions. Table 3 shows the optimized security test results.

Table 3. Optimized Security Test Results

Security testing indicators	Control group 3 (ARIMA+AES encryption)	Control group 4 (LSTM+basic blockchain)	Experimental group (model proposed in this article)	95% confidence interval (experimental group)
Node malicious attack defense success rate (25% malicious nodes)	78.3%	92.5%	98.7%	98.2%-99.2%
Node malicious attack defense success rate (50% malicious nodes)	62.1%	85.8%	94.3%	93.7%-94.9%
Cross node data	Average 286ms,	Average 241ms,	Average 214ms,	Time 206ms-222ms,

encryption transmission (100MB core data)	throughput 389MB/s	throughput 423MB/s	throughput 467mB/s	throughput 455MB/s-479MB/s
Success rate of supply chain privacy data leakage protection	82.5%	93.7%	99.2%	98.9%-99.5%

The experimental group was significantly better than control group 3 and control group 4 in all safety indicators. Among them, the success rate of node malicious attack defense (25% malicious nodes) increased by 6.2 percentage points compared to control group 4 and 20.4 percentage points compared to control group 3, proving that the defense logic combining blockchain consensus mechanism and node verification in this paper has more advantages than traditional encryption and basic blockchain defense. The efficiency of cross node data encryption transmission increased by 11.2% compared to control group 4 and 20.1% compared to control group 3, indicating that the fusion encryption algorithm in this paper not only ensures security but also considers real-time transmission, meeting the real-time interaction needs of the agricultural product supply chain. The success rate of privacy data protection increased by 5.5 percentage points compared to control group 4 and 16.7 percentage points compared to control group 3, highlighting the effectiveness of combining blockchain privacy computing with data anonymization to effectively prevent various privacy leakage risks.

5. Conclusion

This article studies the collaborative application of blockchain and time series analysis in agricultural supply chain security management. Combining the decentralized and tamper proof characteristics of blockchain with the data mining advantages of time series analysis, a collaborative management mechanism is designed and an algorithm model is constructed to address the security needs and pain points of agricultural supply chains. Its effectiveness is verified through experiments. The experiment showed that the accuracy of anomaly detection in this model reached 92% and the recall rate was 88%, which was significantly improved compared to the control group, and could accurately identify risks in each link; The RMSE predicted by key indicators has decreased to 12.5, and the MAE is 9.8, which is close to the true values and provides support for supply chain scheduling decisions. In addition, this technology solution can be adapted to scenarios such as distributed logistics and IoT data management, expanding application boundaries and practical value. This article further clarifies the universal applicability value of the proposed technical solution. The distributed blockchain security mechanism, cross node permission control strategy, and time series anomaly detection model designed in the article are not limited to agricultural supply chain scenarios, but can also be flexibly adapted to other distributed systems. In fields such as distributed logistics monitoring and distributed IoT data management, it can provide important references for solving core security issues such as data tampering, chaotic permissions, and difficult identification of anomalies in general distributed systems, further expanding the application boundaries and practical value of technical solutions.

In the future, research can be deepened from three aspects: firstly, introducing federated learning technology to achieve data privacy computation of blockchain nodes, and solving the contradiction between data sharing and privacy protection. The second is to integrate differential privacy technology, desensitize cross domain shared data, and combine blockchain to build a secure sharing system. The third is to expand the implementation of technical solutions in more distributed scenarios, optimize model parameters, promote the deep integration of the two technologies, and provide more universal and practical security management solutions.

References

[1] Manoj, T., Makkithaya, K., & Narendra, V. G. (2023). A trusted IoT data sharing and secure oracle based access for agricultural production risk management. Computers and Electronics in Agriculture, 204(1), 107544.

[2] Bhat, S. A., Huang, N. F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. Agriculture, 12(1), 40.

[3] Khan, A. A., Shaikh, Z. A., Belinskaja, L., Baitenova, L., Vlasova, Y., Gerzelieva, Z., ... & Barykin, S. (2022). A blockchain and metaheuristic-enabled distributed architecture for smart agricultural analysis and ledger preservation solution: A collaborative approach. Applied Sciences, 12(3), 1487.

[4] Bai, Y., Wu, H., Huang, M., Luo, J., & Yang, Z. (2023). How to build a cold chain supply chain system for fresh agricultural products through blockchain technology—A study of tripartite evolutionary game theory based on prospect theory. Plos one, 18(11), e0294520.

[5] Zheng, Y., Xu, Y., & Qiu, Z. (2023). Blockchain traceability adoption in agricultural supply chain coordination: An evolutionary game analysis. Agriculture, 13(1), 184.

[6] Aldhyani, T. H., & Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. Mathematics, 11(1), 233.

[7] Bai, Y., Fan, K., Zhang, K., Cheng, X., Li, H., & Yang, Y. (2021). Blockchain-based trust management for agricultural green supply: A game theoretic approach. Journal of Cleaner Production, 310, 127407.

[8] Cao, Y., Yi, C., Wan, G., Hu, H., Li, Q., & Wang, S. (2022). An analysis on the role of blockchain-based platforms in agricultural supply chains. Transportation

Research Part E: Logistics and Transportation Review, 163, 102731.

[9] Chen, N., & Li, H. (2024). Agricultural economic security under the model of integrated agricultural industry development. Quality Assurance and Safety of Crops & Foods, 16(3), 25-41.

[10] Si, Y. (2022). Agricultural Cold Chain Logistics Mode Based on Multi - Mode Blockchain Data Model. Computational Intelligence and Neuroscience, 2022(1), 8060765.

[11] Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. IEEE access, 8, 32031-32053.

[12] Mukherjee, A. A., Singh, R. K., Mishra, R., & Bag, S. (2022). Application of blockchain technology for sustainability development in agricultural supply chain: Justification framework. Operations Management Research, 15(1), 46-61.

[13] Bhat, S. A., Huang, N. F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. Agriculture, 12(1), 40.

[14] Vellimalaipattinam Thiruvenkatasamy, K., Ghanimi, H. M., Sengan, S., & Alharbi, M. G. (2025). An online tool based on the Internet of Things and intelligent blockchain technology for data privacy and security in rural and agricultural development. Scientific Reports, 15(1), 27349.

[15] Sayma, M. H., Hasan, M. R., Khatun, M., Rajee, A., & Begum, A. (2024). Detecting the provenance of price hike in agri-food supply chain using private Ethereum blockchain network. Heliyon, 10(11).

[16] Bai, Y., Yang, Z., Huang, M., Hu, M., Chen, S., & Luo, J. (2023). How can blockchain technology promote food safety in agricultural market?—an evolutionary game analysis. Environmental Science and Pollution Research, 30(40), 93179-93198.

[17] Santhanam, E. M., & Kamatchi, K. (2025). Enhancing Agricultural Supply Chain Management With Blockchain Technology and DSA - TabNet: A PBFT - Driven Approach. Transactions on Emerging Telecommunications Technologies, 36(3), e70085.

[18] Zheng, Y., Xu, Y., & Qiu, Z. (2023). Blockchain traceability adoption in agricultural supply chain coordination: An evolutionary game analysis. Agriculture, 13(1), 184.

[19] Ahmed, A., Parveen, I., Abdullah, S., Ahmad, I., Alturki, N., & Jamel, L. (2024). Optimized data fusion with scheduled rest periods for enhanced smart agriculture via blockchain integration. Ieee Access, 12(1), 15171-15193.

[20] Mahalingam, N., & Sharma, P. (2024). An intelligent blockchain technology for securing an IoT-based agriculture monitoring system. Multimedia tools and applications, 83(4), 10297-10320.

[21] Ren, W., Wan, X., & Gan, P. (2021). A double-blockchain solution for agricultural sampled data security in Internet of Things network. Future Generation Computer Systems, 117, 453-461.

[22] Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. IEEE Transactions on Engineering Management, 70(2), 713-739.

[23] Epiphaniou, G., Pillai, P., Bottarelli, M., Al-Khateeb, H., Hammoudesh, M., & Maple, C. (2020). Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security. IEEE Transactions on Engineering Management, 67(4), 1059-1073.