International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 5, Number 1, Year 2025
DOI: https://doi.org/10.62051/ijcsit.v5n1.15
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on the Application of Blockchain Technology in the Field of Agricultural Product Traceability

Jie Zhao [1], Guowei Zhang [1], Xinpeng Miao [1], Fang Liang [2], Peng Zhao [1, *]

[1] School of Computer Science and Technology, Taiyuan Normal University, Jinzhong, 030600, China

[2] Ningbo Vocational and Technical Education Center School, Ningbo City, 315000, China

ABSTRACT

Nowadays, the safety of agricultural products has become an important issue that needs to be solved urgently. Traditional agricultural traceability systems face multiple challenges, including data storage risks, incomplete traceability processes, difficult information traceability, deficiencies in regulatory systems, and lack of consumer oversight. These issues constrain the transparency and credibility of agricultural markets. However, the decentralization and tamper-proof nature of blockchain technology provides an ideal solution for the traceability system of agricultural products, effectively solving the problem of information authenticity and security. This paper discusses the limitations of the traditional agricultural product traceability system, and constructs an agricultural product traceability model and system architecture based on blockchain technology. This paper summarizes the latest research on blockchain technology in the field of agri-food traceability, and analyzes its application progress in five aspects: combining edge computing and cloud technology, enhancing encryption technology, optimizing storage schemes, improving consensus algorithms, and improving smart contract design. By integrating and refining existing research results, it aims to help researchers quickly grasp the essence and latest trends in the field of agricultural product traceability. In addition, it is clearly pointed out that there are still serious challenges in the fields of security, storage and regulation, which opens up a new path and entry point for follow-up research. At the same time, this paper constructs a solid theoretical framework, which provides strong theoretical support and reference for research in related fields.

KEYWORDS

Cryptography; Distributed Storage; Consensus Algorithms; Smart Contracts; Agricultural Product Traceability System

1. INTRODUCTION

Agricultural product traceability systems, as a critical tool for quality supervision, have become an essential safeguard for ensuring food safety [1]. However, traditional agricultural product traceability systems primarily rely on centralized databases to record data, which renders them vulnerable to data tampering, thereby compromising the authenticity and reliability of the information [2]. Centralized systems often lack transparency, making it difficult for consumers and regulatory authorities to access accurate and comprehensive information. Moreover, centralized databases are susceptible to attacks or system failures [3], which can result in the loss of critical information. Consequently, traditional traceability systems face significant challenges in ensuring the security of data storage, highlighting the urgent need for more secure and reliable solutions.

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

As an advanced distributed ledger technology, blockchain offers effective solutions to many challenges faced by traditional traceability systems. By utilizing multi-node data storage, blockchain effectively mitigates the risks of single-point failures and data tampering [4]. All participants share a unified data source, ensuring a high level of transparency and traceability [5]. Once data is recorded on the blockchain, it becomes immutable, guaranteeing data integrity [6]. Furthermore, by integrating encryption technologies and consensus protocols, blockchain ensures secure data storage and effectively prevents unauthorized access attempts [7]. These unique advantages have earned blockchain the title of the "foundation of trust," demonstrating extraordinary potential in addressing trust-related issues inherent in traditional agricultural product traceability systems.

Building on a comprehensive analysis of the problems in traditional agricultural product traceability systems, this study proposes a blockchain-based agricultural product traceability model and its system architecture. The core elements of this model include the following: leveraging IoT devices and sensors to capture real-time information across the production, transportation, and sales stages of agricultural products, which is then recorded on the blockchain to ensure data immutability and transparency; enabling all stakeholders (such as farmers, processing plants, logistics companies, and consumers) to access and verify information in real time to enhance trust; and allowing consumers to easily obtain complete traceability information for agricultural products by scanning QR codes or similar methods. The blockchain-based agricultural product traceability system not only overcomes many shortcomings of traditional systems but also improves the efficiency and credibility of agricultural product quality supervision [8].

This paper summarizes and analyzes the issues in traditional agricultural product traceability systems. Based on the construction of a blockchain-based agricultural product traceability model and its system architecture, it conducts an in-depth study of agricultural product traceability systems leveraging blockchain technology.

2. TRADITIONAL AGRICULTURAL PRODUCT TRACEABILITY SYSTEM ARCHITECTURE

The traditional agricultural food traceability system consists of five fundamental components: data collection, transmission, storage, management, and sharing, as illustrated in Figure 1.

Data from the supply chain is collected using Radio Frequency Identification (RFID) technology and sensor technology [9]. XML is adopted as the data exchange format, and standardized interface technologies provided by Web Services are utilized to transmit the collected data to a centralized database system, ensuring data integrity and consistency through the construction of a central database [10]. Various data processing techniques are employed to clean, organize, deeply analyze, and mine the datasets. Ultimately, diverse service channels, such as online platforms and mobile applications (apps), are used to provide consumers and regulatory agencies with services including traceability inquiries, responsibility tracking, regulatory support, and product recalls.

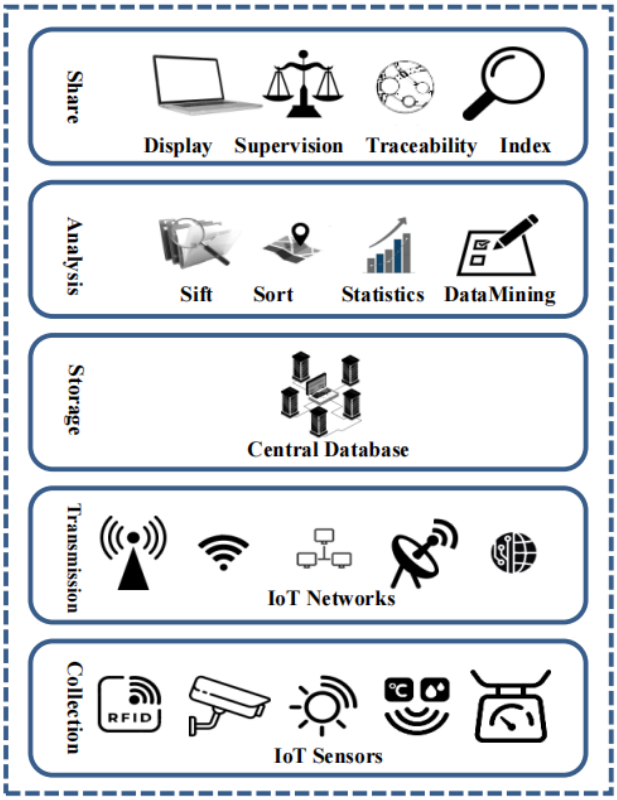

Figure 1. The framework of the traditional traceability system for agricultural products

However, traditional agricultural food traceability systems face multiple issues. Centralized management results in highly concentrated control, making data vulnerable to manipulation and undermining its authenticity. Furthermore, the lack of transparency in agricultural product information creates trust issues. Additionally, the ambiguity in assigning responsibility between trading parties makes it difficult to identify accountable entities [11].

3. BLOCKCHAIN-BASED AGRICULTURAL PRODUCT TRACEABILITY ARCHITECTURE

3.1. Basic Concept of Blockchain

Blockchain technology is a chain-structured data architecture based on timestamps, specifically designed for data storage and verification. At its core, blockchain relies on consensus mechanisms among distributed nodes to manage the creation and updating of data, while employing cryptographic principles to ensure data authenticity and immutability. This establishes a decentralized distributed storage and computation architecture [12]. The introduction of blockchain enables any node within the system to participate in the recording and preservation of information. Even in the event of partial node failure or attempts at fraudulent activity, the overall integrity of the blockchain remains intact, and the information it contains cannot be altered [13].

3.2. Blockchain System Framework

The blockchain system applied to agricultural product traceability primarily consists of a six-layer architecture, as illustrated in Figure 2.

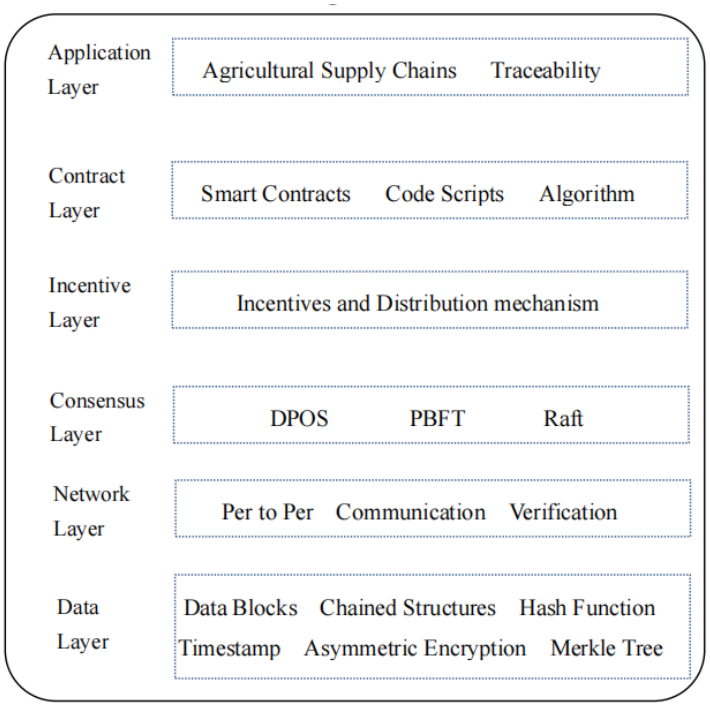

Figure 2. Blockchain architecture for the traceability of agricultural products

Data Layer:The data layer, as the foundational layer of the blockchain, constructs the blockchain's data structure through supporting technologies such as data blocks, chain structures, asymmetric encryption, timestamps, hash functions, and Merkle trees. This layer enables the distributed storage of supply chain data, ensuring data security and immutability [14].

Network Layer:The network layer facilitates network connections and data exchange among blockchain nodes. Its core components include a peer-to-peer (P2P) network architecture, communication protocols, and data validation mechanisms [15]. The P2P network structure promotes efficient information dissemination and sharing, ensuring the real-time accuracy of traceability information while avoiding single-point failures and information delays [16]. This decentralized architecture not only enhances the system's scalability and robustness, allowing it to flexibly accommodate the growing demands of traceability, but also ensures stable operation even in the face of node failures or attacks. Furthermore, the blockchain network layer establishes a fair and transparent information-sharing platform for stakeholders such as producers, processors, logistics companies, retailers, and consumers. This fosters active participation and collaboration among all parties, eliminating information silos and improving the overall efficiency and transparency of supply chain operations [17]. Most importantly, with the support of encryption technologies and distributed ledger architecture, the blockchain network layer ensures the security and privacy of traceability data. Only authorized participants are allowed to access and modify relevant information, effectively preventing the unauthorized disclosure or misuse of sensitive data. This creates a logically sound, secure, and trustworthy agricultural product traceability system.

Consensus Layer:The consensus mechanism ensures that widely distributed nodes within a decentralized environment can agree on the validity of block data, thereby guaranteeing the accurate integration of new blocks into the blockchain architecture [18]. Different blockchain systems typically adopt varying consensus mechanisms based on their specific characteristics. Public blockchains, which have relatively lenient requirements for uniformity and accuracy, generally employ eventual consistency-based consensus mechanisms. In contrast, consortium and private blockchains, which have stricter requirements for uniformity and accuracy, necessitate the use of strong consistency consensus algorithms. Traceability systems utilizing consortium blockchains are capable of resisting malicious attacks and data tampering, ensuring that all participants receive

consistent and reliable traceability information [19]. This not only strengthens consumer trust in the origin and quality of agricultural products but also fosters collaboration and information sharing among supply chain participants.

Incentive Layer:The incentive layer is designed with a framework comprising incentive mechanisms and allocation rules, aimed at encouraging consensus nodes to actively participate in the block generation process. Through competition for bookkeeping rights, the blockchain ledger is continually updated and maintained [20]. The effectiveness of the incentive mechanism significantly enhances the enthusiasm of supply chain members to participate and positively impacts the network's stability.

Contract Layer:Building on the inherent characteristics of blockchain systems—distributed architecture, traceability, and immutability—the introduction of the contract layer significantly improves the system's programmability and flexibility, thereby greatly expanding the application scope of blockchain technology. The core components of the contract layer include programming languages, algorithms, and smart contracts. Smart contracts are jointly established by multiple participants, clearly defining the rights and responsibilities of all parties involved in transactions, and subsequently encoded. These contracts embed specific conditions for triggering terms and the corresponding execution rules [21]. By integrating regulatory mechanisms into the logistics operation process, smart contracts leverage their automatic execution capabilities to generate dynamic QR codes, assigning each item a unique identifier. These codes provide consumers with traceability information, ensuring data reliability.

Application Layer:The application layer enables users to personalize operations by invoking the interfaces of smart contracts within the contract layer. It provides a wide array of application services for diverse participants in the agricultural product supply chain, including product traceability, real-time monitoring, information inquiry, and result visualization.

4. RESEARCH PROGRESS OF BLOCKCHAIN IN AGRICULTURAL PRODUCT TRACEABILITY SYSTEMS

4.1. Integration of Edge-Cloud Technology

Reference [22] demonstrates the effective monitoring of the entire process from seed planting to harvest through the deep integration of blockchain and Internet of Things (IoT) technologies. Sensors and IoT devices eliminate the need for third-party intermediaries by continuously monitoring crop health and environmental conditions. References [23-24] developed a supply chain traceability system based on blockchain and Radio Frequency Identification (RFID) technology, embedding blockchain technology into RFID tags to achieve decentralized data management and ensure data security. References [25-28] proposed a model framework that combines blockchain and IoT technology, optimizing supply chain management efficiency and transparency while enhancing the reliability of product traceability and trust among participants.

The development of edge computing technology has facilitated the formation of a hierarchical distributed architecture that integrates terminal devices, edge networks, and cloud resources. This architecture leverages the low latency and high bandwidth characteristics of edge computing in conjunction with the efficiency of cloud computing. Moreover, the integration of blockchain technology enhances the credibility of data flow and system security. Reference [29] introduced a novel decentralized layered attribute encryption scheme combining edge computing and blockchain. Initially, IoT devices utilize an encryption-based authentication system to verify user access rights in a decentralized manner at the network periphery. Subsequently, edge devices can send data to nearby cloud networks for processing while maintaining privacy. Additionally, users can achieve data sharing through both edge and cloud storage. Using a distributed blockchain network, Reference [30] enables secure communication and authentication between IoT devices supporting edge computing,

as well as between devices and edge servers. References [31-32] accelerated the dissemination of single-signature encrypted messages among target device groups while avoiding reliance on multiple unicast methods.

Reference [33] introduces blockchain technology to enhance the security and privacy of cloud-edge decision-making architecture models and data processing. References [34-35] utilize blockchain technology to provide secure guarantees for data transmission at edge nodes, while also offering decentralized, fine-grained, and dynamic access control management within IoT environments. References [36-37] proposed a blockchain-based decentralized proactive caching strategy in mobile edge computing environments, addressing the limited storage capacity of edge nodes and the issue of malicious behavior. Furthermore, based on the trust of edge servers, a trust relationship is established between content providers and edge servers to safeguard the caching process. Reference [38] involves re-encrypting data resources at edge nodes before storage, ensuring both transaction security and the dual protection of user privacy and resources.

4.2. Enhanced Encryption Technologies

In blockchain-based supply chain frameworks, sensitive data involving personal privacy or commercial secrets undergoes desensitization measures such as anonymization and de-identification to ensure that original information cannot be restored. For critical traceability data that must be retained, encryption algorithms are employed to protect the data from unauthorized interpretation and utilization. Fine-grained access control strategies are developed based on the roles and needs of different participants. One privacy protection solution for blockchain involves utilizing zero-knowledge proofs (zk-SNARK) and attribute-based encryption (ABE) to support multi-level supervision. Reference [39] employs zk-SNARKs to hide users' transaction addresses and values within an account model. Subsequently, by adopting attribute-based encryption, a multi-level supervision model is established while implementing privacy protection measures that allow selective disclosure of transaction content. Reference [40] enables participants to enter the system using one-time pseudonyms, thus protecting their identity information. The use of attribute encryption technology secures product information stored on the blockchain, while smart contracts establish flexible access control strategies for encrypted product information. Reference [41] combines public key encryption schemes with zk-SNARKs to ensure that user identities remain undisclosed, while also designing a two-layer commitment structure to achieve fine-grained privacy protection (identity anonymity and data confidentiality) and flexible data state transitions.

Furthermore, the construction of agricultural product traceability systems presents risks associated with counterfeit and substandard products. Therefore, it is essential to clearly define the responsibilities of each participant to prevent and minimize potential disputes.Reference [42] proposes a blockchain-based supply chain framework utilizing a combination of symmetric and asymmetric key encryption to achieve privacy protection. Product owners can not only trace their products but also transfer ownership. Reference [43] introduces a linkable ring signature (LRS) scheme to ensure the traceability of all transaction records related to the same cold chain product. Finally, Reference [44] employs a chameleon hash function to facilitate data modification capabilities, enabling the correction of erroneous data and updating of data access permissions while maintaining a record of data modifications on the blockchain, thereby establishing an accountability mechanism to identify malicious entities.

4.3. Optimization of Storage Methods

With the rapid advancement of Internet of Things (IoT) technologies, numerous sensors have been widely integrated across various stages of the supply chain, generating a substantial amount of traceable data. This data encompasses a variety of media forms, including but not limited to images,

videos, and text. However, the necessity for each blockchain node to retain complete data increases storage burdens and limits enhancements in network performance.

The optimization of blockchain storage can be primarily categorized into on-chain and off-chain strategies. On-chain strategies involve storing data within the chain structure of the blockchain, including techniques such as sharding to alleviate storage burden, index optimization to enhance retrieval speed, lightweight nodes to reduce redundancy, and multi-chain architectures to expand capacity. Off-chain strategies, on the other hand, entail migrating data to external distributed systems, such as peer-to-peer storage architectures utilizing distributed hash table technology, cloud storage based on the InterPlanetary File System (IPFS) for data compression, or leveraging edge computing capabilities to offload part of the data storage and processing to edge devices near the data source, thereby reducing storage pressure on central nodes.

Reference [45] introduced a dual-chain storage architecture for blockchain aimed at optimizing data management in food supply chains. This architecture comprises a main chain that stores complete data and a summary chain that retains data summaries. Nodes can select storage methods according to their needs, effectively alleviating storage pressure on the main chain and significantly optimizing the utilization of storage resources. Reference [46] proposed horizontal and vertical partitioning when designing blocks. The header and body of the blockchain are stored separately, with the body stored in IPFS. The data can be segmented based on time or size; when new blocks are added, miners only need to copy the latest portion and append the tail and vertical segments. This design strategy effectively addresses the challenges related to storage efficiency and scalability faced by traditional blockchain technologies. Reference [47] proposed a hybrid storage architecture integrating blockchain and IPFS that employs cryptographic techniques to achieve the separation of public and private data storage. Public data is stored on the blockchain, while private data is retained in IPFS, aiming to alleviate the storage burden of the blockchain and enhance query efficiency. Farm data is recorded in IPFS, with its hash stored in smart contracts, effectively addressing the storage capacity issues of blockchain. Reference [48] introduced a blockchain storage framework tailored for agricultural IoT data, utilizing adaptive lossy compression techniques to differentiate between normal and abnormal data and implement corresponding compression strategies. This aims to enhance the value density of on-chain data, significantly reducing storage space and optimizing the storage efficiency of the blockchain.

However, in the face of the challenges posed by massive spatiotemporal data in the IoT era, it is essential to improve data storage and access efficiency, reduce storage costs, and enhance system scalability and security to meet the practical application requirements of agricultural product traceability. Reference [49] proposed a layered sharding blockchain storage model, employing a master-slave structure that deploys the main chain in a cloud center, integrating the state information of multiple shard subchains, with each shard subchain responsible for data storage. Additionally, subchains are designed at the edge chain layer to aggregate edge devices with similar performance, thereby enhancing data storage and access efficiency. Reference [50] presented an enhanced lightweight node model (ESPV) that utilizes block classification storage management, sharding storage, and hierarchical access technologies to optimize storage costs while ensuring the security and decentralization of the system, thereby enhancing scalability to accommodate more agricultural product data. Reference [51] proposed a scalable blockchain storage solution based on block encoding compression, which improves system scalability by reducing the storage requirements and read overhead for full nodes, making it more suitable for high-frequency data updates and query demands.

4.4. Improvement of Consensus Mechanisms

Consensus algorithms are the core mechanisms governing the operation of blockchain networks, responsible for ensuring the consistency and security of the entire network. These algorithms define the processes for block creation and validation, while delineating the responsibilities and rights of

nodes within the network. They establish rules for selecting block creators to ensure fairness and enhance network security and resilience against attacks through the penalization of malicious behaviors [52].

Public chains, consortium chains, and private chains select different types of consensus algorithms based on their respective application scenarios and requirements. This targeted selection of consensus algorithms ensures optimal performance of blockchain networks across various contexts. Reference [53] proposed an improved Delegated Transparent Byzantine Mask (DTBM) DPoS consensus algorithm, which employs the K-means algorithm to pre-select reliable nodes in the delegation queue, thereby enhancing node reliability. The donation process is transparent and traceable, increasing the system's openness and public trust. This effectively overcomes potential centralization issues inherent in traditional DPoS algorithms, thereby strengthening system security. Reference [54] presented a new model of the Practical Byzantine Fault Tolerance (PBFT) algorithm based on consortium chains. This model enhances resilience against malicious nodes through credit evaluation and the WtC consensus mechanism while significantly improving system performance and fault tolerance, showcasing promising application prospects. Reference [55] introduced a secure and efficient consensus algorithm, the Verifiable Secret Sharing Byzantine Fault Tolerance Raft Consensus Algorithm (VSSB-Raft). The VSSB-Raft algorithm employs zero-trust mechanisms, data authentication, and communication optimization to maintain efficiency while also achieving Byzantine fault tolerance, making it applicable in blockchain or distributed systems requiring high security and reliability.

Agricultural product traceability systems typically adopt a consortium chain architecture. However, due to the risks of conflicts of interest and malicious behaviors in consortium chain environments, PBFT-based consensus algorithms have become the preferred choice for applications such as agricultural product traceability. Nevertheless, PBFT algorithms face several challenges, including significant communication overhead and poor scalability [56]. Consequently, research efforts aimed at improving PBFT algorithms seek to better align them with the application needs of blockchain technology. Reference [57] proposed a novel Proof of Transaction (PoTx) consensus algorithm designed to achieve scalability by reducing communication overhead and computational requirements. This algorithm enhances system fault tolerance by selecting random validators from the consensus group based on transaction counts. Reference [58] introduced an improved consensus algorithm that reduces the volume of network data transmission during the node consensus process, exhibiting superior throughput and latency compared to the Considerations algorithm, thereby enhancing consensus efficiency and alleviating communication bottlenecks. Reference [59] proposed a Credit Evaluation-based Practical Byzantine Fault Tolerance (CE-PBFT) algorithm. This algorithm designs a new node credit evaluation model that considers node completion rates, consensus degradation, and node behaviors, effectively measuring and reflecting the reliability of nodes throughout the system's operational process, thus enhancing system reliability and security.

4.5. Improvement of Smart Contract Design

Smart contracts operate automatically in a trusted environment, managing access and data privacy according to predetermined terms [60]. This automated execution mechanism enhances computational determinism and reduces subjective judgment during data processing, making smart contracts widely adopted in agricultural product traceability systems. Reference [61] introduced a novel framework that combines consortium chains with smart contracts, allowing farmers to store critical information such as environmental parameters and crop growth data in the IPFS distributed storage system while recording the corresponding IPFS hash values in smart contracts. This framework ensures data security while fully leveraging the distributed characteristics of IPFS, effectively alleviating the storage pressure faced by the blockchain. Reference [62] proposed an organic rice supply chain traceability framework based on consortium chains and smart contracts, achieving secure data storage and full traceability and information sharing throughout the supply

chain through customized data management strategies and smart contracts, effectively addressing challenges related to data privacy protection and traceability.

Current research focuses on two areas: on one hand, improving the execution processes of smart contracts to create efficient and secure tracking systems; on the other hand, expanding the functionalities of smart contracts based on tracking requirements to enhance security and maintainability, thereby effectively managing supply chain data. Reference [63] constructed a dynamic regulatory model framework based on blockchain and smart contract technologies, embedding three specific types of smart contracts: initialization contracts, model verification contracts, and credit evaluation contracts. This framework aims to enhance the reliability and transparency of supply chain data and leverage algorithms to verify model feasibility. Reference [64] implemented an Attribute-Based Access Control (ABAC) model through smart contracts, designing smart contracts for each component of the model to achieve automated management of edge intelligent data resources and fine-grained access control. References [65-67] extended the functional forms of smart contracts to improve their development efficiency as well as security and maintainability, thereby better meeting traceability business needs. References [68-70] optimized smart contracts to address potential security vulnerabilities, thereby enhancing the security and reliability of blockchain smart contracts.

5. DISCUSSION

This paper conducts a comprehensive review of the application of blockchain technology in the field of agricultural product traceability through bibliometric and content analysis. The results indicate that the integration of blockchain with agricultural food supply chains is a prevailing trend in the industry; however, challenges remain in the application of blockchain technology for product traceability.

5.1. Data Security Issues

The data layer serves as the foundation of the blockchain architecture, encapsulating core data and encryption algorithms to ensure the robust operation and security of the blockchain. Although complex encryption technologies safeguard data immutability and privacy, issues such as user key leakage persist. To mitigate this risk, the implementation of multi-signature technology is recommended, allowing multiple keys to jointly sign transactions, thereby enhancing the security of transactions and the overall stability and reliability of the blockchain system.

Within the blockchain technology framework, the network layer relies on core functional modules such as peer-to-peer (P2P) network technology, information dissemination protocols, and data validation mechanisms to ensure the legitimacy and equality of participation of all nodes in the consensus mechanism and ledger maintenance process. This layer is foundational for the circulation of information within the blockchain; however, the integration of multiple technologies also introduces security risks. To prevent risks such as P2P network attacks, it is advisable to restrict access to unauthorized nodes, enhance monitoring of network anomalies, and appropriately adjust connection parameters to ensure network security and stability.

Smart contract technology enables users to establish customized transaction rules among multiple parties, ensuring that all participating nodes adhere to the same code logic during transaction execution on the blockchain. This technology exhibits significant advantages in terms of security, customizability, and economic efficiency. However, the immutability of smart contracts means that any existing vulnerabilities could lead to severe security issues. To mitigate such risks, regular code audits should be conducted, and professional security teams should be engaged to thoroughly examine the smart contract code to identify and rectify potential security vulnerabilities.

5.2. Storage and Scalability Issues

As the user base and transaction volume continue to rise, the agricultural product traceability system increasingly faces challenges regarding massive data storage efficiency and system scalability. First, the accumulation of extensive historical data can elevate storage costs. Second, transaction throughput may become a bottleneck, limiting system performance. Furthermore, as the blockchain system expands, a singular chain structure may struggle to meet the demands of data growth, potentially obstructing real-time recording and verification of data.

To address these issues, it is recommended to implement a hierarchical strategy within the system architecture to achieve decoupling of functional modules, thereby reducing system complexity. Additionally, employing sidechain and multichain technologies allows for the migration of certain data to sidechains while recording hash values on the main chain, effectively alleviating the storage burden on the main chain. Considering the unique characteristics of the various entities involved in the supply chain, a distributed blockchain network architecture should be designed to avoid the concentration of transaction data on a single chain, thereby enhancing system processing efficiency. Lastly, the application of sharding technology can segment the network into multiple independent zones, which not only reduces the workload of individual nodes but also enhances the system's concurrent processing capabilities.

5.3. Traceability and Regulatory Issues

The agricultural food supply chain system that employs blockchain technology faces numerous regulatory challenges.

First, cross-border regulation encounters difficulties. Given that the agricultural food supply chain involves multiple countries and regions, discrepancies in regulatory standards and legal frameworks present a core issue for effective cross-border collaborative regulation. Therefore, there is an urgent need for unified technical specifications in the industry to ensure the effective implementation of regulatory measures.

Second, although blockchain technology ensures data immutability, verifying the authenticity and accuracy of the original data remains a challenge. This necessitates the use of deep learning algorithms to identify and rectify data issues, as well as the establishment of data review mechanisms to verify the credibility of data sources.

Moreover, the current integration of blockchain technology with existing regulatory frameworks has not yet reached an ideal state, prompting regulatory bodies to actively seek innovative regulatory frameworks. This includes strengthening specialized training on blockchain regulatory technologies and their applications to promote the co-evolution of regulatory models and blockchain technology, particularly through the implementation of a new management model termed "on-chain regulatory chains." Establishing a "rule of law chain," leveraging the transparency of blockchain, can effectively identify and promptly respond to potential security risks. Furthermore, the comprehensive network record retention and decentralized trust mechanisms of blockchain significantly enhance regulatory efficiency, enabling the regulatory system to dynamically update and effectively address the limitations of traditional policy regulation, thereby improving the entire regulatory framework.

6. CONCLUSION

Blockchain technology, characterized by decentralization, immutability, and distributed storage, demonstrates substantial application potential in the field of agricultural product traceability. This paper analyzes the issues inherent in traditional agricultural product traceability systems and proposes a model architecture for traceability systems based on blockchain technology. A comprehensive analysis is conducted on the application of blockchain technology in conjunction with edge

computing and cloud technologies, enhanced encryption techniques, optimized storage solutions, improved consensus algorithms, and refined smart contract design across five dimensions pertinent to agricultural product traceability. By analyzing existing research outcomes, this paper aids researchers in rapidly acquiring core knowledge and the latest developments in this field. Additionally, it highlights significant challenges that remain in the areas of security, storage, and regulation, providing new directions and entry points for future research. Finally, a theoretical framework is established to support and reference related studies.

REFERENCES

[1] Ying LIU, Hongbo FAN, Shouqun MA, Zhiwei GAO, Jinjiang LIU. Blockchain based trusted traceability system scheme for raw milk supply chain [J]. Telecommunications Science, 2021, 37(5): 148-159.

[2] Chen Jinwen, Luo Decun, Tang Chengjun, Tang Chenjun, Ding Yong. Blockchain-based trusted traceability system for agricultural Internet of Things [J]. Chinese Journal of Information Security, 2022, 7(2):139-149.

[3] Wan Shixian, Zhao Yu, Wu Chengrong. Evaluation and empirical evidence of network attack resistance of mimic database [J]. Computer Applications and Software, 2022, 39(01):319-327.

[4] LUO Cheng. Research on the Construction of Scientific Research Security Supervision and Management System in Colleges and Universities Based on Blockchain Technology [J]. Electronic Communications and Computer Science, 2024, 6(7): 157-159.

[5] Tan Pengliu, Xu Teng, Yang Sijia, et al. A review of blockchain privacy protection technology [J]. Computer Application Research, 2024, 41(08):2261-2269.

[6] YAO Yuan. Research on Data Security Sharing Methods of Enterprise Fintech from the Perspective of Blockchain Technology [J]. Journal of International Economics & Management, 2023, 4(5): 112-114.

[7] Research Progress of Blockchain in the Field of Data Security [J]. Chinese Journal of Computers, 2021, 44(1): 1-27.

[8] Wang Minxue, Li Bo, Wen Shuning, et al. A Review and Analysis of Blockchain Technology Empowering Food Supply Chain Traceability [J]. Journal of University of Electronic Science and Technology of China (Social Sciences Edition), 2023, 25(2): 42-54.

[9] Research Progress on the Application of Intelligent Packaging Technology in Food Supply Chain [J]. FOOD SCIENCE, 2021, 42(7): 336-344.

[10] ZHANG Jianguo. Discussion on the Application of Data Integration in Enterprise Supply Chain Management [J]. Electronic Communications and Computer Science, 2024, 6(4): 145-147.

[11] ZHANG Honghong. Research on the Risks and Prevention of Rural E-commerce Development in China from the Perspective of Law [J]. E-Commerce Review, 2024, 13(3): 5164-5171.

[12] XU Xinmei. Design of Data Storage and Transfer System Based on Blockchain Technology [J]. Electronic Communications and Computer Science, 2023, 5(5): 185-187.

[13] Wu Xiaotong, Liu Pingzeng, Wang Zhihua. Research on Traceability System of Agricultural Products Based on Blockchain [J]. Computer Applications and Software, 2021, 38(5): 42-48.

[14] CHENG Junchao, ZHANG Chi, HE Yuanan. Application of blockchain technology in cross-departmental marine data sharing [J]. Science & Technology Review, 2020, 38(21): 60-68.

[15] Kang Bohan, Zhang Ning, Zhu Jianming. Cross-chain Service Framework and Communication Mechanism of Intelligent Service Transactions Based on Blockchain [J]. Chinese Journal of Network and Information Security, 2021, 7(3): 105-114.

[16] Si Bingru, Xiao Jiang, Liu Cunyang, et al. Overview of Blockchain Network [J]. Journal of Software, 2023, 35(2): 773-799.

[17] SUN Guoqiang, XIE Yufei. blockchain technology, Supply Chain Network and Data Sharing: Based on the Perspective of Evolutionary Game [J]. CMS, 2024, 31(12): 149-162.

[18] ZHU Jianming, ZHANG Qinnan, GAO Sheng. Research Progress on Key Technologies and Applications of Blockchain [J]. Journal of Taiyuan University of Technology, 2020, 51(3): 321-330.

[19] ZHANG Zhao, TIAN Jixin, JIN Ching-qing. on-chain evidence, Trusted Data Sharing Platform for Off-chain Transmission [J]. Big Data Research, 2020, 6(5): 106-117.

[20] SHEN Chuan-nian. Review on security issues of blockchains [J]. Computer Engineering & Science, 2024, 46(01): 46-62.

[21] Yunting S, Chao S. Legal Intervention: Judicial Remedies for Smart Contract Disputes [J]. Journal of Beijing University of Aeronautics and Astronautics Social Sciences Edition, 2023, 36(6): 70-79.

[22] Hasan H R, Musamih A, Salah K, et al. Smart agriculture assurance: IoT and blockchain for trusted sustainable produce [J]. Computers and Electronics in Agriculture, 2024, 224: 109184.

[23] Miao F, Tian P B, Tao B, et al. Design of agricultural product traceability system based on blockchain and RFID [J]. 2024.

[24] Wang L, He Y, Wu Z. Design of a blockchain-enabled traceability system framework for food supply chains [J]. Foods, 2022, 11(5): 744.

[25] Nair A, Peddibhotla U, Chandran S C, et al. Convergence of IoT and Blockchain Ecosystem to Ensure Traceability and Reliability in Agricultural Supply Chain[C]//2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2024: 388-390.

[26] Brandín R, Abrishami S. IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing [J]. Automation in Construction, 2024, 159: 105266.

[27] Lu Y, Li P, Xu H. A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things [J]. Procedia Computer Science, 2022, 199: 629-636.

[28] Leteane O, Ayalew Y. Improving the Trustworthiness of Traceability Data in Food Supply Chain Using Blockchain and Trust Model [J]. The Journal of The British Blockchain Association, 2024.

[29] Sasikumar A, Ravi L, Devarajan M, et al. Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things [J]. IEEE Access, 2024.

[30] Zhang S, Cao D. A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT [J]. The Journal of Supercomputing, 2024, 80(5): 6778-6808.

[31] Mollah M B, Azad M A K, Zhang Y. Secure Targeted Message Dissemination in IoT Using Blockchain Enabled Edge Computing [J]. arXiv preprint arXiv: 2401.06384, 2024.

[32] Shi L, Wang T, Xiong Z, et al. Blockchain-aided Decentralized Trust Management of Edge Computing: Towards Reliable Off-chain and On-chain Trust [J]. IEEE Network, 2024.

[33] Chi C, Yin Z, Liu Y, et al. A trusted cloud-edge decision architecture based on blockchain and mlp for aiot [J]. IEEE Internet of Things Journal, 2023, 11(1): 201-206.

[34] Zhonghua C, Goyal S B, Rajawat A S. Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing [J]. The Journal of Supercomputing, 2024, 80(2): 1396-1425.

[35] Yao Y, Chang J, Zhang A. Efficient Data Sharing Scheme With Fine-Grained Access Control and Integrity Auditing in Terminal-Edge-Cloud Network [J]. IEEE Internet of Things Journal, 2024, 11(16): 26944-26954.

[36] Bai J, Zhu S, Ji H. Blockchain Based Decentralized and Proactive Caching Strategy in Mobile Edge Computing Environment [J]. Sensors, 2024, 24(7): 2279.

[37] Bounaira S, Alioua A, Souici I. Blockchain-enabled trust management for secure content caching in mobile edge computing using deep reinforcement learning [J]. Internet of Things, 2024, 25: 101081.

[38] Huang W, Yu X, Ma Z. A Study on Blockchain-Based Data Proxy Re-Encryption Privacy Protection[C]//2024 3rd International Conference on Cryptography, Network Security and Communication Technology. 2024: 25-29.

[39] Jia W, Xie T, Wang B. A privacy-preserving scheme with multi-level regulation compliance for blockchain [J]. Scientific Reports, 2024, 14(1): 438.

[40] Li J, Wang Z, Guan S, et al. ProChain: A privacy-preserving blockchain-based supply chain traceability system model [J]. Computers & Industrial Engineering, 2024, 187: 109831.

[41] Jiang Z L, Xie M, Chen H, et al. RPSC: Regulatable Privacy-Preserving Smart Contracts on Account-based Blockchain [J]. IEEE Transactions on Network Science and Engineering, 2024, 11(5): 4822-4835.

[42] Mohit, Kaur S, Singh M. Design and implementation of blockchain-based supply chain framework with improved traceability, privacy, and ownership [J]. Cluster Computing, 2024, 27(3): 2345-2363.

[43] Zhang Y, Tang Y, Li C, et al. Privacy-preserving for Blockchain-enabled Cold-chain Logistics System with IoV and Linkable Ring Signature [J]. IEEE Transactions on Vehicular Technology, 2024, 73(9): 12585-12596.

[44] Yang S, Li S, Chen W, et al. A Redactable Blockchain-Based Data Management Scheme for Agricultural Product Traceability [J]. Sensors, 2024, 24(5): 1667.

[45] GAO S, LIU X, GAO Y. Optimized model of dual-chain storage of food supply chain data based on blockchain [J]. Food and Machinery, 2023, 36(11): 63-70.

[46] Wang Z, Wang L, Xiao F, et al. A traditional Chinese medicine traceability system based on lightweight blockchain [J]. Journal of medical Internet research, 2021, 23(6): e25946.

[47] Babu S, Devarajan H. Agro-food supply chain traceability using blockchain and IPFS [J]. International Journal of Advanced Computer Science and Applications, 2023, 14(1):393-399.

[48] JING Xu,SHI Yindi. Transactions of the CSAE,2024,40(02):273-282.

[49] Li C, Pan H, Qian H, et al. Hierarchical sharding blockchain storage solution for edge computing [J]. Future Generation Computer Systems, 2024, 161: 162-173.

[50] ZHAO Yulong, NIU Baoning, LI Peng, et al. Blockchain-enhanced lightweight node model [J]. Journal of Computer Applications, 2020, 40(04):942-946.

[51] XIAO Heling, GUO Wangmei, WANG Jing. Distributed Coding Scheme for Blockchain Based on Regenerative Code [J]. Journal of Jilin University(Engineering Science), 2022, 52(11): 2685-2697.

[52] Wang Tianzhu, Li Ling, Peng Zhichen, et al. Design of traceability framework for trusted manufacturing supply chain based on blockchain [J]. Computer Application Research, 2024, 41(05):1308-1313.

[53] Liu W, Li Y, Wang X, et al. A donation tracing blockchain model using improved DPoS consensus algorithm [J]. Peer-to-Peer Networking and Applications, 2021, 14: 2789-2800.

[54] Tan J, Goyal S B, Singh Rajawat A, et al. Anti-Counterfeiting and Traceability Consensus Algorithm Based on Weightage to Contributors in a Food Supply Chain of Industry 4.0 [J]. Sustainability, 2023, 15(10): 7855.

[55] Tian S, Bai F, Shen T, et al. Vssb-raft: a secure and efficient zero trust consensus algorithm for blockchain [J]. ACM Transactions on Sensor Networks, 2024, 20(2): 1-22.

[56] LI Junji, ZHANG Jiaqi. Improved PBFT consensus algorithm based on reputation mechanism [J]. Application Research of Computers, 2024, 41(06):1628-1634.

[57] Saranya P, Maheswari R. Proof of transaction (PoTx) based traceability system for an agriculture supply chain [J]. IEEE Access, 2023, 11: 10623-10638.

[58] Xie Z, Kong H, Wang B. Dual-Chain Blockchain in Agricultural E-Commerce Information Traceability Considering the Viniar Algorithm [J]. Scientific Programming, 2022, 2022(1): 2604216.

[59] Xiao J, Luo T, Li C, et al. CE-PBFT: A high availability consensus algorithm for large-scale consortium blockchain [J]. Journal of King Saud University-Computer and Information Sciences, 2024, 36(2): 101957.

[60] Liu Shaojie, Zhao Hongbo, Liu Xun. Trusted Blockchain Automation Protocol Based on Domain Programming Model [J]. Journal of Applied Sciences, 2024, 42(4): 569-584.

[61] Wang L, Xu L, Zheng Z, et al. Smart contract-based agricultural food supply chain traceability [J]. Ieee Access, 2021, 9: 9296-9307.

[62] Shannan L, Changzheng L, Ronghua Z, et al. Research on organic rice traceability based on blockchain smart contract [J]. Journal of Chinese Agricultural Mechanization, 2024, 45(1): 217.

[63] Peng X, Zhang X, Wang X, et al. Construction of rice supply chain supervision model driven by blockchain smart contract [J]. Scientific Reports, 2022, 12(1): 20984.

[64] He G, Li C, Shu Y, et al. Fine-grained access control policy in blockchain-enabled edge computing [J]. Journal of Network and Computer Applications, 2024, 221: 103706.

[65] Marchesi L, Mannaro K, Marchesi M, et al. Automatic generation of ethereum-based smart contracts for agri-food traceability system [J]. Ieee Access, 2022, 10: 50363-50383.

[66] Reddy C V K, Yatheendra K, AnilKumar T. ETHEREUM-BASED SMART CONTRACTS FOR AGRI-FOOD TRACEABILITY STRUCTURE TO AUTOMATIC GENERATING CODE [J]. UGC Care Group I Listed Journal, 2023, 13(9):109-117.

[67] Valencia-Payan C, Griol D, Carlos Corrales J. Blockchain self-update smart contract for supply chain traceability with data validation [J]. Logic Journal of the IGPL, 2024: jzae047.

[68] Chen Hong, Wang Yinghui, Jin Haibo, et al. Research on DoS vulnerability optimization of smart contract for blockchain auction refund transaction [J]. Application Research of Computers, 2023, 40(02):343-348.

[69] CHEN Jinfu, WANG Zhenxin, CAI Saihua, et al. Vulnerability Detection Method of Blockchain Smart Contract Based on Transformation Test [J]. Journal on Communications, 2023, 44(10): 164-176.

[70] QIAN Peng, LIU Zhenguang, HE Qinming, et al. Research on Security Vulnerability Detection Technology of Smart Contract [J]. Journal of Software, 2021, 33(8): 3059-3085.