Differential Privacy-Enhanced Rice Blockchain Quality Control Model Postprint

Authors: Wu Guodong, Hu Quanxing, Liu Xu, Qin Hui, Gao Bowen

Date: 2024-08-30T00:00:00+00:00

Abstract

[Purpose/Significance] To address issues in traditional rice quality supervision and traceability systems, including imperfect quality control data chain mechanisms, insufficient traceability of quality control information, low data-on-chain efficiency, and privacy information leakage, a differential privacy-enhanced rice blockchain quality control model is proposed. [Method] First, by integrating the entire rice industry chain, a data transmission process is designed to cover stages including planting, procurement, processing, storage, and sales, thereby effectively ensuring the continuity of the quality control data chain. Second, to resolve the issues of large data volumes and low on-chain storage efficiency, key quality control data from each stage of the rice industry chain is stored in the InterPlanetary File System (IPFS), with only the hash values returned after storage being uploaded to the blockchain. Finally, to enhance the traceability of quality control information, privacy-sensitive portions of key quality control data from the planting stage are processed using Differential Privacy before being presented to users, thereby obfuscating individual data, improving the credibility of quality control information, and protecting the privacy of farmers' cultivation data. Based on this quality control model, a differential privacy-enhanced rice blockchain quality control system was designed and deployed in operational rice enterprises. [Results and Discussion] Experimental results demonstrate that the system achieves an average storage time of 1.125 s for single-stage data throughout the entire industry chain, and an average information traceability query time of 0.691 s. Compared with traditional rice quality supervision and traceability systems, single-stage data storage time is reduced by 6.64%, and information traceability query time is reduced by 16.44%. Conclusion The proposed model not only enhances the continuity of quality control data and the degree of information traceability while protecting farmers' privacy, but also improves, to a certain extent, the efficiency of quality control data storage and information traceability queries, offering a valuable reference for the design and improvement of rice quality supervision and information

traceability systems.

Full Text

Differential Privacy-enhanced Blockchain-Based Quality Control Model for Rice

WU Guodong[1,2]*, HU Quanxing[1,2], LIU Xu[3,4], QIN Hui[1,2], GAO Bowen[1,2]

[1]College of Information and Artificial Intelligence, Anhui Agricultural University, Hefei 230036, China
[2]Anhui Provincial Key Laboratory of Smart Agriculture Technology and Equipment, Hefei 230036, China
[3]Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu 610041, China
[4]University of Chinese Academy of Sciences, Beijing 100049, China

Abstract:
[**Objective**] Rice plays an indispensable role in daily diet, and consumer concerns about its quality issues continue to grow, with increasing emphasis on selecting high-quality, safe, and healthy rice. However, the rice market suffers from information asymmetry and uneven quality, causing consumer distress. Traditional rice quality supervision and traceability systems face problems such as incomplete quality control data chain mechanisms, insufficient traceability of quality control information, low data on-chain efficiency, and privacy information leakage. This study proposes a differential privacy-enhanced blockchain-based quality control model for rice to address these challenges. [**Methods**] First, combining the entire rice industry chain, we designed a data transmission process covering cultivation, acquisition, processing, warehousing, and sales to effectively ensure the continuity of the quality control data chain. Second, to solve the problems of large data volume and low on-chain efficiency, key quality control data from each link of the rice industry chain was stored in the InterPlanetary File System (IPFS), and the returned hash value was then uploaded to the blockchain. Finally, to improve the traceability of quality control model information, the sensitive portions of key cultivation data were processed through differential privacy before being presented to users, obfuscating individual data to enhance the credibility of quality control information while protecting farmers' cultivation privacy. Based on this quality control model, we designed a differential privacy-enhanced rice blockchain quality control system and implemented it in actual rice enterprises. [**Results and Discussion**] Testing showed that the differential privacy-enhanced rice blockchain quality control system completed single-link data storage in an average of 1.125 seconds and information traceability queries in an average of 0.691 seconds. Compared with traditional rice quality supervision and traceability systems, single-link data storage time was reduced by 6.64%, and information traceability query time was reduced by 16.44%. [**Conclusions**] The proposed model not only improves

quality control data continuity and information traceability but also protects farmers' privacy. Additionally, it enhances the efficiency of quality control data storage and information traceability queries, providing a reference for the design and improvement of rice quality supervision and information traceability systems.

Keywords: IPFS; blockchain; quality control; efficient on-chain; differential privacy enhancement; information traceability

---

Rice plays an indispensable role in daily diet, and consumer attention to its quality issues continues to increase, with greater emphasis on selecting high-quality, safe, and healthy rice. However, the rice market suffers from information asymmetry and uneven quality, causing consumer distress [1,2]. To meet consumer demands and ensure rice quality reliability, domestic and foreign scholars have conducted extensive research on optimizing rice supply chains, product information traceability, and standardizing rice processing and production. For example, Qian et al. [3] studied rice quality supervision and traceability systems, demonstrating the relationship between supply chain information and product traceability. Liu et al. [4], Wang et al. [5], and Zhang et al. [6] proposed methods combining blockchain technology to improve data security and credibility in the rice industry system. These studies have promoted the sustainable development of the rice industry. However, current research on rice quality supervision and traceability systems still has shortcomings, as it fails to adequately address the mutually supportive relationship between quality control and traceability functions. While traceability can make product information visible to a certain extent, it cannot directly guarantee product quality. Strengthening quality control measures can not only ensure product quality but also indirectly enhance the credibility of traceability functions [7,8].

Traditional rice quality supervision and traceability systems have defects in the continuity of quality control information chains. The information chain related to the rice industry chain is often incomplete or lacks important links, significantly reducing the credibility of rice quality control and traceability information. Additionally, traditional systems lack detailed statistics and display of cultivation-related quality control data, resulting in insufficient product information traceability [9,10]. Information such as pesticide usage, which significantly impacts rice product quality, is particularly important. Second, the rice traceability process faces security issues such as privacy information leakage that urgently need to be addressed [11,12]. Furthermore, to ensure data immutability, the common practice of uploading all product information completely to the chain leads to high blockchain storage costs [13,14].

Rice product traceability information primarily originates from quality control data across the entire industry chain, which directly affects the authenticity and reliability of traceability information. Therefore, quality control is crucial for the traceability process, and product traceability can also serve as part of the

quality control process. To address the problems faced by current rice quality supervision and traceability systems, this study proposes a differential privacy-enhanced blockchain-based quality control model for rice. Its data transmission process covers cultivation, acquisition, processing, warehousing, and sales, ensuring the continuity of rice quality supervision and traceability data chains. Relevant data required for each link of the rice industry chain is stored in IPFS, and the returned IPFS hash value is stored on the blockchain. This approach solves the bottleneck problem of high costs associated with uploading large data to the chain in traditional data on-chain processes. To improve the traceability of rice product information, collected cultivation data—including soil information and agricultural chemical usage—is processed using differential privacy technology for information involving farmer privacy before being displayed to consumers. The quality control model integrates the entire rice industry chain, specifically analyzes and improves the data transmission process, emphasizes the mutually supportive relationship between rice quality control and information traceability, and provides new solutions for optimizing traditional rice quality supervision and traceability systems.

1.1 Blockchain Technology

Blockchain technology is a cryptography and distributed system-based technology that enables decentralized, tamper-proof, transparent, and secure data exchange and storage through distributed consensus mechanisms, blockchain data structures, and smart contracts [15]. The blockchain structure is shown in Figure 1 [Figure 1: see original paper]. It connects blocks in a chain to ensure data continuity and integrity [16]. The distributed consensus mechanism ensures that nodes in the network reach consensus on transactions [17], while smart contracts allow automatically executable contract logic to be executed without third-party intervention [18]. This gives blockchain broad application potential in finance, supply chain management, healthcare, and other fields, providing new solutions for building trust, improving efficiency, and promoting innovation [19,20]. This study proposes a differential privacy-enhanced blockchain-based quality control model for rice based on blockchain technology and implements systematic design and development on the Ethereum platform.

1.2 InterPlanetary File System

IPFS is a decentralized distributed file storage and transmission protocol designed to solve data storage and transmission problems in the traditional internet [21]. Its storage principle is based on content addressing, using a unique Content Identifier (CID) to locate and retrieve files. In IPFS, files are divided into data blocks, and a unique CID is generated through a hash function, representing the hash of the file content rather than its location. This means files can be located through their unique content identifier without relying on specific servers or storage locations. IPFS uses a Distributed Hash Table (DHT) to store and locate file blocks, with each node storing part of the hash table.

It finds nodes containing the CID through the CID in the network and obtains file blocks through a distributed protocol [22]. This distributed storage mechanism increases file availability and redundancy, improving file reliability and download speed.

1.3 Differential Privacy Technology

Differential privacy is a privacy protection technology used to protect individual sensitive information during data publishing or analysis [23]. It adds noise to query results, datasets, or algorithm outputs [24], making it impossible for attackers to accurately infer individual sensitive information. The mathematical definition of differential privacy can be expressed as: for any two adjacent datasets D and D', and any query function Q (mapping of query results), differential privacy requires that for any output S and any privacy attacker's background knowledge K, formula (1) is satisfied.

The rice industry chain involves numerous enterprises in cultivation, acquisition, processing, warehousing, and sales. However, information silos exist between these links, lacking effective quality control data interaction, which easily leads to uncertainty in quality management and product traceability. Therefore, establishing a complete and continuous traceable link quality control data chain is crucial. It not only helps ensure stable product quality but also enhances the credibility of information traceability, providing stronger support for the healthy development of the entire industry chain. Through data sharing and integration, each link can collaborate more closely, strengthen quality management, improve overall efficiency, and thereby enhance consumer confidence in product quality and safety. As shown in Table 1 , based on the analysis of key quality control data in the rice industry chain, classified according to industry chain links and data traceability, after completing the information on-chain storage process for each link, publicly available quality control data can directly serve as product traceability information. Information involving farmer privacy in the cultivation link is processed through differential privacy before being displayed, improving product information traceability while protecting farmer privacy. Private quality control data that consumers cannot trace, such as costs in each link, is limited to internal sharing within relevant enterprises.

2.2 Model Overall Architecture

Based on blockchain, IPFS, and other technologies, combined with differential privacy technology, this study designs a differential privacy-enhanced blockchain-based quality control model for rice. As shown in Figure 2 [Figure 2: see original paper], its core idea is to integrate the entire rice industry chain including cultivation, acquisition, processing, warehousing, and sales to solve the problem of incomplete quality control data chains in rice product quality supervision and information traceability. Additionally, through blockchain, IPFS, and differential privacy technologies, the model improves the traceability of rice product information while ensuring the efficiency and privacy security

of data storage and sharing across the entire industry chain, achieving comprehensive optimization and improvement of the rice blockchain quality control model.

The overall architecture can be divided into four layers: IoT device layer, industry chain system layer, IPFS layer, and blockchain layer. In the IoT device layer, sensors and related devices collect detailed data during the rice cultivation process, including humidity, temperature, lighting, and pesticide usage. After completing key data collection, they upload it to the cloud in real time. The industry chain system layer stores link-specific key quality control data and generates a unique cultivation information ID, which serves as the head of the information chain in the rice industry chain. This layer manages and tracks the rice production process, storing and managing relevant data from cultivation, acquisition, processing, warehousing, and sales, and building a reliable information chain for rice quality control and traceability. The cultivation information ID and related data are stored in the cultivation module of the industry chain system, with subsequent modules storing the unique number from the previous link, forming a reliable information chain that plays a key role in rice quality control. To solve the overhead problem caused by large data volumes, after completing data storage, each link uploads key quality control data to the corresponding IPFS node through its API. Finally, the returned hash value is integrated and stored in the blockchain network, completing the on-chain process for industry chain data. Additionally, combining differential privacy technology, information involving farmer privacy in the cultivation module (such as pesticide usage) is processed and displayed to consumers through visualization technology, while information like fertilizer amount can directly supplement product traceability information. This collaborative architecture among IoT devices, industry chain systems, IPFS, and blockchain builds a reliable and secure data supervision and traceability system, optimizing data storage and sharing efficiency, solving information chain mechanism deficiencies and farmer privacy leakage problems in rice quality supervision and traceability, and improving rice product traceability, enabling consumers to trust and understand the origin and quality of purchased rice products.

2.3 Model Data Flow Design

As shown in Figure 3 [Figure 3: see original paper], based on the differential privacy-enhanced blockchain quality control model, the data flow for rice industry chain quality control is designed by combining various layers in the model.

After IoT devices complete comprehensive data collection, key quality control data is transmitted to the cloud and then stored in the cultivation module of the rice industry chain system, including detailed cultivation-related data collected by various sensors and devices such as environmental information. When the rice industry chain system completes information storage for each link, key quality control data is uploaded to the corresponding IPFS node in real time. By dividing data into blocks and storing them distributedly, data reliability

and persistence are ensured, and other nodes can quickly retrieve and access data. To ensure the integrity and immutability of rice industry chain data, the hash value returned from storing link data in IPFS is verified through the hash-on-chain smart contract deployed on the blockchain (such as hash number verification) before being uploaded to the rice consortium chain. Cultivation nodes, acquisition nodes, processing nodes, warehousing nodes, and sales nodes represent relevant participants in the consortium chain [28]. In the smart contract, an access control mechanism is established for different roles such as cultivators, acquirers, and processors. By verifying node identity identifiers, each participant can only access and process data related to their role. This design ensures that only authorized nodes can access and process role-specific data, preventing participants from obtaining sensitive information from other links and thereby protecting data privacy and security. When storing cultivation traceability data requiring differential privacy processing, the privacy budget is preset based on evaluations of general parameters by cultivation enterprises and relevant research institutions. When users trace rice product information, they scan the packaging QR code or use the rice industry chain system. Based on the traceability query smart contract, after verifying link hash integrity, they obtain the IPFS hash value of the corresponding product, retrieve the corresponding traceability information from IPFS, and simultaneously trigger the differential privacy protection mechanism. According to the preset privacy budget value, partial cultivation data is processed before returning the product traceability information.

In this model's data flow design, link-specific key quality control data in the industry chain is uploaded to IPFS, and the returned hash value is verified through the hash-on-chain contract before being uploaded to the blockchain. This ensures the continuity of rice quality supervision and traceability data chains while improving data on-chain efficiency and system operation. When users trace product information, differential privacy processing technology introduces noise into partial cultivation data, making individual privacy information unidentifiable while maintaining overall data characteristics to ensure data usability. This protects farmers' cultivation-related sensitive data while still enabling users to obtain in-depth product traceability information, meeting user needs while avoiding farmer privacy leakage and further enhancing the practicality of the quality control model.

2.4 Data Privacy Protection Design

To solve the problem of insufficient product information traceability in traditional rice quality supervision and traceability systems, the quality control model integrates with the entire rice industry chain to display detailed indicator statistics from the rice cultivation stage to users. However, direct display may lead to leakage of farmers' sensitive information. Therefore, this study adopts differential privacy technology to process returned cultivation traceability data during user traceability queries. By adding noise to partial data, it ensures

that farmers' private individual information cannot be reverse-engineered or identified. Finally, processed pest control information is displayed through visualization technology to reflect data distribution and changes. The introduction of differential privacy solves the challenge of displaying sensitive data in information traceability, providing possibilities for establishing a more transparent rice quality control model.

The specific differential privacy protection process for traceable quality control data in the cultivation link is shown in Figure 4 [Figure 4: see original paper].

1) When users trace rice product information, partial information from the cultivation link is processed through differential privacy before statistical display. First, parameter parsing is performed on cultivation link traceability data to review the structure and content of the original dataset, understanding its source and purpose. Second, various fields in the dataset are identified, recording field names, meanings, and data types. For numerical fields, value ranges and units are understood; for text fields, formats and encoding methods are comprehended. Third, relationships and dependencies between fields are analyzed to understand correlations. Finally, parameter parsing results are organized and returned to lay the foundation for subsequent differential privacy processing and statistical display.

2) If dataset fields do not involve farmer privacy, original data is returned. If fields involve farmer privacy, the Laplace mechanism is applied for differential privacy processing to generate a privacy dataset.

3) Finally, the privacy dataset processed through differential privacy is merged with the public dataset to generate privacy-protected cultivation traceability data, which is returned to users together with traceability data from other links.

After parameter parsing of the original cultivation traceability dataset, the Laplace mechanism is used to perturb the data. The perturbation process satisfies -differential privacy. The specific steps for differential privacy processing of cultivation traceability data are as follows:

1) To ensure high product information traceability, comprehensive traceability of rice is performed to display cultivation traceability information from all supplying farmers for the batch of products. After parameter parsing, the relevant dataset requiring privacy protection is obtained. This dataset contains n cultivation farmers, denoted as $P = \{p_1, p_2, \ldots, p , \ldots, p \}$, where p represents the i-th cultivation farmer, and i satisfies $1 \leq i \leq n$. The batch of rice requires privacy protection for m types of information, denoted as $I = \{info_1, info_2, \ldots, info , \ldots, info \}$, where info represents the j-th type of information requiring privacy protection for this rice variety, and j satisfies $1 \leq j \leq m$. For these n farmers supplying the rice variety used in this batch, privacy protection processing will be applied to m types of related cultivation information.

2) The j-th type of rice privacy cultivation information recorded by the i-th farmer p is represented as d , and a privacy cultivation information matrix D × is constructed. This matrix contains traceable privacy cultivation information recorded by farmers supplying the rice used in this batch, where n is the number of farmers and m is the number of categories of privacy cultivation information for this rice variety.

3) Based on the privacy protection cultivation information matrix D × , a noise matrix N × with the same number of rows and columns is generated. When element d in D × is valid, the noise element n in row i and column j follows a Laplace distribution, satisfying n = Laplace(Δd/), where Laplace() is the random generation function for Laplace noise [29]; Δd is global sensitivity, with Δd = max(d) - min(d); is the privacy parameter, where smaller values indicate stronger privacy protection [25], but may lead to loss of data usability. The privacy parameter value needs to be adjusted based on specific data to balance privacy security and data usability.

4) In differential privacy, the probability density function of the Laplace distribution satisfies formula (2):

f(x|e, s) = (1/2s) × exp(-|x - e|/s)

where x is a random variable; e is the expectation of variable x; s is the scale parameter of variable x. In the Laplace mechanism, e = 0, and the variance of this distribution satisfies $\sigma^2 = 2s^2$, where s = Δd/ .

The noise matrix N × is added to the cultivation information matrix D × to obtain the perturbed cultivation information matrix D' × , satisfying D' × = {d' = d + n , d D × , n N × }. The element d' in row i and column j of the perturbed cultivation information matrix D' × satisfies formula (4):

d' = d_{min}, d' ≤ d_{min} d' , d_{min} < d' < d_{max} d_{max}, d' ≥ d_{max}

where d_{max} is the upper bound of cultivation information and d_{min} is the lower bound. By limiting the amount of noise added, the usability of perturbed cultivation information is improved, ensuring data does not exceed the original range, thereby guaranteeing data reliability to a certain extent while protecting privacy.

The main processing steps can be represented by Algorithm 1.

Algorithm 1: Differential Privacy Protection for Cultivation Traceability Data

Input: Sensitive traceability dataset data, privacy budget privacy_{budget}
Output: Privacy-protected data protected_{data}

```
1 Function LaplaceMechanism(data, sensitivity, ):
2     scale = sensitivity /    // Calculate noise scale
```

```
3     noise = Laplace(0.0, scale, size=data.shape)  // Generate Laplace noise
4     noisy_{data} = data + noise  // Add noise
5     return noisy_{data}

6 Function ApplyDifferentialPrivacy(data, ):
7     param_{values} = ExtractParameterValues(data)  // Data processing
8     sensitivity = Max(param_{values}, axis=0) - Min(param_{values}, axis=0)  // Calculate
9     noisy_{{{param}}_{{values}}} = LaplaceMechanism(param_{values}, sensitivity, )  // La
10    data = noisy_{{{param}}_{{values}}}
11    return data

12 Function ApplyDifferentialPrivacyWithBudget(data, privacy_{budget}):
13    protected_{data} = ApplyDifferentialPrivacy(data.copy(), privacy_{budget})
14    return protected_{data}
```

Original data example: - Farmer: zhang** - Pesticide usage (g(mL)/667m^2): 375.63, 350.25, 386.34, 323.22, 315.89 - Soil alkali-hydrolyzable nitrogen content (mg/kg): [values] - Planting density (10,000 holes/hm^2): [values]

3.1 System Overall Architecture Design

Based on the quality control model, we designed a differential privacy-enhanced blockchain-based quality control system for rice, with its architecture shown in Figure 5 [Figure 5: see original paper]. The system architecture can be divided into physical layer, transport layer, storage layer, service layer, and application layer according to specific functions. The physical layer, as the bottom layer of the system architecture, involves sensor devices and network infrastructure, responsible for ensuring data collection from all links of the industry chain, including temperature, humidity, and gas concentration data, providing a reliable data foundation for upper layers. The transport layer is responsible for data transmission and communication, using various communication protocols and technologies including the Internet, LAN, and Bluetooth to upload data collected from the physical layer to the cloud, while encrypting and compressing data to ensure security and efficiency during transmission. The storage layer consists of traditional databases, IPFS, and blockchain, which work together to achieve efficient on-chain and off-chain storage and management of system key data. Traditional databases are used for structured data management and querying, IPFS stores key quality control data from industry chain links, and blockchain stores the hash values returned by IPFS. This integrated storage approach improves system operation efficiency and ensures the continuity, reliability, and traceability of quality control data in the rice system, providing consumers with trustworthy rice quality control information. The service layer bears important responsibilities in the system architecture, mainly handling business logic and providing functional services, including receiving user requests, performing data validation and authorization, etc. The function implementation of the application layer mainly relies on a series of API designs

in the service layer. The top layer of the system architecture is the application layer, responsible for providing user-oriented functions and interfaces, covering Web applications, mobile applications, etc., for system data display and functional interaction to meet various needs including quality inspection and certification, user and product management, rice product sales, rice product information traceability, and departmental supervision.

3.2 System Implementation

Based on the above system architecture design, this study implemented a differential privacy-enhanced blockchain-based quality control system for rice, which has been practically applied in relevant rice enterprises in Lu'an City, Anhui Province, effectively solving problems such as insufficient quality control data storage continuity, low on-chain efficiency, insufficient product information traceability, and farmer privacy leakage in rice enterprises and traditional rice industry chains. In each link of the rice industry chain, numerous IoT devices are needed to collect and upload information in real time to ensure the safety and efficient operation of the industry chain. Figure 6 [Figure 6: see original paper] shows some IoT devices used in the physical layer of the system. Figure 6a shows a grain condition monitoring substation, used for real-time monitoring of temperature, humidity, gas concentration, and other parameters in rice warehouses or storage facilities, performing intelligent control and adjustment based on this data to ensure safe storage and good quality of rice. Figure 6b shows a rice processing monitoring station, which can monitor and control real-time steps and status during rice processing. Figure 6c shows a grain heavy metal analyzer, used for detecting and analyzing heavy metal content in rice.

The bottom layer of the system architecture provides necessary infrastructure and functional services for the application layer to support upper-layer applications and implement specific business requirements. Figure 7 [Figure 7: see original paper] shows some system-related applications. Figure 7a displays the monitoring homepage of the quality control system backend, which can show real-time blockchain-related information such as on-chain enterprises, block transactions, smart contracts, and total block count. It can also view real-time data feedback from sales clients, enabling enterprises to achieve comprehensive management and monitoring of all industry chain links. Figure 7b shows the Web backend information traceability query page, facilitating enterprises to inspect and trace relevant rice quality control information and obtain key information from all links of the rice industry chain. Among these, partial traceability information from the cultivation link is processed through differential privacy and finally presented to consumers in statistical view form. Figure 7c shows the traceability page on mobile devices, where consumers can trace product information through rice packaging numbers or QR codes, displaying traceability information from all links including cultivation, acquisition, processing, warehousing, and sales, consistent with the Web backend traceability query information.

3.3 System Testing and Analysis

This system was developed based on Ethereum client Geth v1.12.1, using the Proof of Work (POW) mechanism, with programming languages including Java, Solidity, and Javascript. The system was deployed using a combination of Alibaba Cloud servers and offline physical servers, relying on the bastion host protection environment of the physical servers to build an internal network for project access. This architecture fully utilizes the elasticity and flexibility of Alibaba Cloud servers while leveraging the security and stability of physical servers. In specific configuration, the Alibaba Cloud server uses 8-core 64 GB hardware configuration, 20 Mbps bandwidth, and Ubuntu 20.04 LTS operating system to better support Docker containerization technology and other open-source technologies. Additionally, the internal network uses Zerotier technology to connect Alibaba Cloud servers and physical servers virtually, achieving secure internal network connections.

During product information traceability, the introduction of differential privacy protection mechanisms prevents farmer privacy leakage but impacts query performance to a certain extent. To verify whether the differential privacy-enhanced rice blockchain quality control system ensures the efficiency of industry chain data storage and traceability queries while securely improving product information traceability through differential privacy technology, we tested the time required for storing key quality control data from all links including cultivation, acquisition, processing, warehousing, and sales, as well as the time required for product information traceability queries. To ensure rigorous and authentic experimental results, we compared it with traditional blockchain storage and query-based rice blockchain quality supervision and traceability models, conducting 200 tests for industry chain link data storage efficiency and 200 tests for product information traceability query efficiency each.

In the experiments, test data was selected from key quality control data of all links in the industry chain for a specific rice product from an enterprise in Lu'an City. The improved method's storage process includes storing key quality control data in traditional databases, uploading it to IPFS by module, and storing the returned link hash value in the rice blockchain. Each storage contains 58 quality control parameter information items. The traceability query result includes traceable data from key quality control data, with each query containing 40 quality control parameter information items, among which sensitive traceability information is processed through differential privacy. In the traditional model, key quality control data is uploaded directly from traditional databases to the blockchain for storage testing. In traceability query testing, privacy traceability data is displayed as general traceability parameter visualization for quantitative comparison with the improved model.

Taking the average of every 20 test results as one data point, as shown in Figure 8 [Figure 8: see original paper], the improved system completed whole industry chain data storage in an average of 5.623 seconds, with single-link

storage averaging 1.125 seconds. The traditional single-chain storage method completed whole industry chain data storage in an average of 6.025 seconds, with single-link storage averaging 1.205 seconds. The improved method reduced single-link storage time by 6.64%. This demonstrates that using IPFS hash values for on-chain storage instead of direct data upload can effectively solve the delay problem caused by large data uploads.

As shown in Figure 9 [Figure 9: see original paper], with the introduction of the differential privacy algorithm, the improved method's rice product information traceability query averaged 3.456 seconds, while the traditional model averaged 4.136 seconds, representing a 16.44% reduction in query time. This shows that the method combining blockchain and IPFS can effectively compensate for the query performance loss caused by differential privacy processing in the rice quality control model, and to some extent improves information traceability query efficiency, confirming the applicability of differential privacy protection mechanisms in rice quality control models.

Conclusion

To address problems in traditional rice quality supervision and traceability systems such as incomplete quality control information chain mechanisms, insufficient traceability, low data on-chain efficiency, and privacy leakage, this study proposes a differential privacy-enhanced blockchain-based quality control model for rice. Combining the entire rice industry chain, we designed a data transmission process covering cultivation, acquisition, processing, warehousing, and sales, effectively ensuring the continuity of quality control data chains. On this foundation, the blockchain-IPFS storage mode solves problems of large data volume and low efficiency in traditional on-chain storage. Finally, to improve product information traceability, sensitive cultivation data is processed through differential privacy protection and displayed to users through visualization technology, improving traceability while protecting individual farmers' cultivation privacy.

Based on the quality control model, we designed a differential privacy-enhanced rice blockchain quality control system. Through practical operation in relevant rice enterprises, the system demonstrates improved continuity and traceability of rice quality control information while effectively protecting farmer privacy. In terms of rice key quality control data storage and information traceability query efficiency, the system completes single-link data storage in an average of 1.125 seconds and information traceability queries in an average of 0.691 seconds. Compared with traditional rice blockchain quality supervision and traceability models, single-link data storage time is reduced by 6.64% and information traceability query time by 16.44%, achieving good results that can provide reference for the design and improvement of rice industry chain quality control systems.

Conflict of Interest Statement: This study has no conflicts of interest among researchers or with publicly published research results.

References

[1] TAO Q, CAI Z Y, CUI X H. A technological quality control system for rice supply Chain[J]. Food and energy security, 2023, 12(2): ID e382.
[2] ZHANG Q Y, LI T P. Study on the rice and safety in China[J]. Cereals & oils, 2022, 35(11): 143-146.
[3] QIAN L L, ZUO F, ZHANG C D, et al. Geographical origin traceability of rice: A study on the effect of processing precision on index elements[J]. Food science and technology research, 2019, 25(5): 619-624.
[4] LIU S N, LIU C Z, ZHANG R H, et al. Research on organic rice traceability based on blockchain smart contract[J]. Journal of chinese agricultural mechanization, 2024, 45(1): 217-222, 251.
[5] WANG L, REN J R, WANG T, et al. Design and implementation of food security traceability system based on blockchain[J]. Science technology and engineering, 2023, 23(4): 1625-1634.
[6] ZHANG Y, WU X Y, GE H Y, et al. A blockchain-based traceability model for grain and oil food supply chain[J]. Foods, 2023, 12(17): ID 3235.
[7] BIAN L P, LYU Y, LUO Z B, et al. Application conception and design of food traceability in the Metaverse based on blockchain technology[J]. Journal of intelligent agricultural mechanization, 2023, 4(4): 11-19.
[8] LIANG H, LIU S C, ZHANG Y N, et al. Multi-blockchain application technology for agricultural products transaction[J]. Smart agriculture, 2019, 1(4): 72-82.
[9] GAO Y Y, LYU X W, Y L, et al. Application of blockchain-based trusted traceability of agricultural products[J]. Computer applications and software, 2020, 37(7): [pages].
[10] WANG M X, LI B, WEN S N, et al. Reviewing analysis on traceability in food supply chain empowered by blockchain technology[J]. Journal of UESTC (social sciences edition), 2023, 25(2): 42-54.
[11] LI T M, YAN X, ZHANG Z N, et al. Application research of blockchain+internet of things in agricultural product traceability[J]. Computer engineering and applications, 2021, 57(23): 50-60.
[12] ZHA K J, WANG Z B, HE Y S, et al. Review on blockchain security protection[J]. Computer and modernization, 2023(6): 110-117.
[13] SINGH A, GUTUB A, NAYYAR A, et al. Redefining food safety traceability system through blockchain: Findings, challenges and open issues[J]. Multimedia tools and applications, 2023, 82(14): 21243-21277.
[14] SI B R, XIAO J, LIU C Y, et al. Survey on blockchain network[J]. Journal of software, 2024, 35(2): 773-799.
[15] GUO H Q, YU X J. A survey on blockchain technology and its security[J]. Blockchain: Research and applications, 2022, 3(2): ID 100067.
[16] FAN X, NIU B N, LIU Z L. Scalable blockchain storage systems: Research progress and models[J]. Computing, 2022, 104(6): 1497-1524.
[17] WANG X Y, YIN S R. Research on Database Storage Technology based on Consensus Mechanism[C]// Proceedings of the 2nd International Conference on Bigdata Blockchain and Economy Management. Hangzhou, China: EAI,

2023.
[18] PENG X Z, ZHAO Z Y, WANG X Y, et al. A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends[J]. Computers and electronics in agriculture, 2023, 208: ID 107834.
[19] ZHAO Y D, LI Q D, YI W L, et al. Agricultural IoT data storage optimization and information security method based on blockchain[J]. Agriculture, 2023, 13(2): ID 274.
[20] BALCERZAK A P, NICA E, ROGALSKA E, et al. Blockchain technology and smart contracts in decentralized governance systems[J]. Administrative sciences, 2022, 12(3): ID 96.
[21] ATHANERE S, THAKUR R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing[J]. Journal of king Saud university-computer and information sciences, 2022, 34(4): [pages].
[22] CHEN H D, FENG Y X, NIU Y H. Industrial internet data trusted storage system based on IPFS blockchain technology[J]. Computer science and application, 2022, 12: ID 1292.
[23] WANG T, HUO Z, HUANG Y X, et al. Review on privacy-preserving technologies in federated learning[J]. Journal of computer applications, 2023, 43(2): 437-449.
[24] WU X T, QI L Y, GAO J Q, et al. An ensemble of random decision trees with local differential privacy in edge computing[J]. Neurocomputing, 2022, 485: 181-195.
[25] ADNAN M, KALRA S, CRESSWELL J C, et al. Federated learning and differential privacy for medical image analysis[J]. Scientific reports, 2022, 12: ID 1953.
[26] SARKAR A, SHARMA A, GILL A, et al. A differential privacy-based system for efficiently protecting data privacy[C]// 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). Piscataway, New Jersey, USA: IEEE, 2023: 1399-1404.
[27] VASA J, THAKKAR A. Deep learning: Differential privacy preservation in the era of big data[J]. Journal of computer information systems, 2023, 63(3): 608-631.
[28] LI J T, HAN D Z, WU Z D, et al. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control[J]. Future generation computer systems, 2023, 142(C): 195-211.
[29] WU Q T, LI M W, ZHU J L, et al. DP-RBAdaBound: A differentially private randomized block-coordinate adaptive gradient algorithm for training deep neural networks[J]. Expert systems with applications, 2023, 211: ID 118597.

Note: Figure translations are in progress. See original paper for figures.