applied sciences

Article

Research on the Trusted Traceability Model of Taishan Tea Products Based on Blockchain

Kangchen Liu [1,2], Pingzeng Liu [1,2,3,*] and Shuaishuai Gao [1,2]

[1] School of Information Science and Engineering, Shandong Agricultural University, Taian 271018, China
[2] Key Laboratory of Huang-Huai-Hai Smart Agricultural Technology, Ministry of Agriculture and Rural Affairs, Taian 271018, China
[3] Agricultural Big-Data Research Center, Shandong Agricultural University, Taian 271018, China
[*] Correspondence: pzliu@sdau.edu.cn

Abstract: In recent years, the rapid development of the Taishan tea industry has become a business card of local specialty agriculture. However, as consumers' demands for Taishan tea product quality and safety continue to improve, the centralized database traceability system that the traditional Taishan tea industry relies on shows insufficient information credibility and core data security risks, making it difficult to match the diversified expectations of the market and consumers. In order to solve this problem, this paper proposes a trusted traceability model for Taishan tea based on blockchain technology, which utilizes blockchain technology and data hierarchical uploading mechanism to ensure data accuracy and transparency, and, at the same time, improves data uploading efficiency. The optimized SM2 encryption algorithm is introduced, and the execution efficiency of the encryption algorithm is improved by the concurrent processing framework, which guarantees the security and transmission speed of the data. The experimental results show that the blockchain-based trusted traceability model for Taishan tea significantly improves the data security, query, and writing speed, and greatly optimizes the problems of traditional traceability methods. With this research, the results in this paper not only help to improve the quality and safety of Taishan tea products but also provide technical support for the production enterprises to enhance their brand competitiveness.

Keywords: Taishan tea; traceability model; blockchain; encryption algorithm

Citation: Liu, K.; Liu, P.; Gao, S. Research on the Trusted Traceability Model of Taishan Tea Products Based on Blockchain. *Appl. Sci.* **2024**, *14*, 10630. https://doi.org/10.3390/app142210630

Academic Editor: Luis Javier Garcia Villalba

Received: 22 August 2024
Revised: 19 September 2024
Accepted: 21 September 2024
Published: 18 November 2024

1. Introduction

Tea is a beverage widely enjoyed around the globe and occupies a pivotal position in Chinese culture, nourishing people's material lives as well as profoundly influencing their spiritual pursuits. Among them, Taishan tea has a long history and is an important part of tea culture. In recent years, the Taishan tea industry has flourished, formed a large-scale, intensive industrial pattern, become an important driving force for the development of local agriculture, and attracted much attention.

With the increasing prominence of food quality and safety issues, tea, as a popular beverage, and the construction of its traceability system, has become the focus of widespread consumer concern. A study summarized the methods of tea sample pre-treatment and pesticide residue detection, elaborated the migration pattern and influencing factors of pesticide residues during tea planting and processing, conducted a risk assessment and traceability of pesticide residues in tea, and proposed improvement strategies [1]. Another study investigated the evaluation of blockchain-based traceability by consumers in the tea industry in China and summarized it, which helps to help consumers recognize the value of blockchain-based traceability technology [2]. Some have summarized the progress of the application of smart technologies in the tea industry, analyzed the existing challenges and gaps, and proposed future research trends [3]. In terms of outlier processing in tea traceability data, a study proposed an unsupervised outlier detection mechanism to effectively ensure the quality of tea traceability data [4].

In our in-depth exchanges and cooperation with Taishan tea enterprises, we have observed that although the Taishan tea industry is booming at an unprecedented rate, behind it lies the core challenges of insufficient informatization service capacity of the Taishan tea industry, lack of supervision of the production process, and low information security in the planting and production process. These problems directly restrict the Taishan tea industry from further adapting to the diversified demands of the market, especially the difficulty in meeting the high concern of contemporary consumers for high-quality, personalized tea products and food safety. For this reason, we propose to integrate blockchain technology into the Taishan tea industry, design and construct a trusted traceability model for Taishan tea based on blockchain, and enhance the credibility and market competitiveness of the Taishan tea brand.

In the process of in-depth cooperation and communication with Taishan tea enterprises, we have organized a series of visits and research activities to comprehensively and meticulously understand the whole chain traceability process of Taishan tea from source to market. Based on the valuable information from the field research, we designed a set of traceability programs in line with the characteristics of the Taishan tea industry and constructed the Taishan tea traceability model. Through researching the Taishan tea industry chain, we clarified the information content of Taishan tea traceability, constructed the Taishan tea traceability process and traceability structure, and drew them into the form of pictures and tables for people to browse. In order to ensure the authenticity and extensiveness of the traceability data, we utilize the IoT devices installed in Taishan tea enterprises to collect real-time and accurate industry chain data covering all aspects of the Taishan tea industry. In the data processing stage, we followed the random sampling principle to select data samples to ensure the general applicability and unbiasedness of the experimental results. Next, we used the traditional SM2 encryption algorithm and the optimized SM2 encryption algorithm and showed the flow of SM2 before and after optimization in the form of a flowchart, and then derived the experimental results. The experimental results show that the optimized SM2 encryption algorithm exhibits significant advantages in encryption efficiency, decryption speed, and security and has superior performance compared with the traditional algorithm. This finding not only verifies the effectiveness of the optimized algorithm but also provides solid technical support for the data security of the Taishan tea traceability model.

Aiming at the centralized database architecture challenges currently faced by Taishan tea-related enterprises, including inefficient data processing and slow data writing and accessing, this study innovatively introduces blockchain technology. Blockchain stores data in a network consisting of multiple nodes instead of a single centralized server of a traditional database. This approach realizes distributed storage of data, reduces the load pressure on a single server, and improves data availability and fault tolerance. By implementing the blockchain solution and combining it with a hierarchical data upload strategy, we have significantly enhanced our data processing capabilities and realized efficient data flow and instant access. In order to verify the actual effect of this upgrade, we have carefully designed several experiments and strictly selected the results of one of them for presentation. The experimental results show that the blockchain-based Taishan tea trusted traceability model shows significant advantages in data security, transparency, and traceability efficiency compared with the traditional model, which not only effectively improves consumer trust, but also lays a solid technical foundation for the high-quality development of the Taishan tea industry. This change not only solves the bottleneck problem of the original system but also opens up a new path for the strengthening of Taishan tea's brand reputation and market expansion.

This model is carefully designed for the traceability of Taishan tea products, fully considering the uniqueness and traceability needs of the Taishan tea industry; however, it does not mean that its principle and technical architecture are limited to the field of Taishan tea. In fact, the research on blockchain-based traceability of agricultural products has been quite extensive, covering numerous categories of agricultural products. Yang, X.T. et al. designed a traceability system based on blockchain technology and applied it to fruits and vegetables [5]. Xiao, F. et al. developed a novel traceability mechanism using sharding technology to support easier traceability operations of traditional Chinese medicines [6]. Varavallo, G. et al. designed a traceability platform based on a green blockchain, which is low in energy consumption, and cost-saving for the cheese supply chain [7]. Salah, K. et al. designed an efficient execution of business transactions using Ethernet blockchain and smart contracts for soybean tracking and tracing throughout the agricultural supply chain [8]. López-Pimentel, J.C. et al. combined the advantages of traditional data traceability with a microservices architecture and added a new blockchain-auditing layer, and applied this technology to the Mexican avocado supply chain [9]. Guan, S.P. et al. proposed a new blockchain-based model for agricultural product traceability systems, which has good versatility and can protect the privacy of agricultural product information in the traceability system [10].

2. Research Status of Tea Information Traceability and Blockchain Technology

2.1. Tea Information Traceability Related Content

Xu, X.F. et al. introduced blockchain and IoT technologies into the field of tea to realize the whole process of traceability and automatic environmental control to ensure the safety, reliability, and efficiency of the agricultural product traceability system [11]. Wu, Y.T. et al. analyzed the whole process of a tea supply chain from planting to sales, constructed the system architecture and various functions, and designed and implemented a machine learning blockchain-IoT-based tea Trusted Traceability System [12]. Paul, T. et al. studied the incorporation of blockchain technology into the tea supply chain, which extends the resource-based view and network theory and helps to develop a more sustainable supply chain for the global tea industry [13]. Another study has developed a distributed and service-oriented system architecture for the tea industry network that helps to manage the complex circular tea supply chain management and establish transparency and traceability in the industry [14].

Huang, Y.T. et al.'s study revealed small-scale tea farmers' perceptions of a national traceability platform, further expanding the scope of current research on farmer behavior [15]. Chen, C.L. et al. study specifically applies the distributed theory and service-oriented ideas to the tea supply chain system model, introduces the interstellar file system technology to store the tea traceability data, solves the data incremental problem in the process of tea production, and realizes the anti-counterfeiting traceability of the tea supply chain of a regulatory nature [16].

2.2. Blockchain Technology and Crypto-Related Content

Zou, Y.P. et al. proposed a blockchain-assisted multi-keyword fuzzy search encryption scheme for secure data sharing, which supports fine-grained access control and attribute revocation and ensures the reliability of the search process [17]. Xu, G.X. et al. proposed an encryption scheme combining blockchain technology and certificate-less encryption, which not only enables the certificate-less encryption scheme to withstand the two kinds of attacks but also reduces the storage space of the blockchain and solves the complex certificate management problem [18]. Liu, L. et al. used federated blockchain technology and updated homomorphic encryption to generate the data structure of encrypted blocks and implement the updated encryption algorithm for big data privacy [19]. Liang, W. et al. built a mathematical model based on homomorphic encryption by utilizing the blockchain and smart contracts and designed the algorithm, including the blockchain generation, homomorphic chain encryption and decryption, and smart contracts, which improves the efficiency of data storage and supervision [20]. Feng, T. et al. combined hierarchical attribute encryption with linear ciphertext sharing, and proposed a blockchain data privacy protection control scheme based on searchable attribute encryption, which solves the problem of privacy exposure in traditional blockchain transactions [21]. Du, R.Z. et al. proposed a dynamic searchable encryption scheme using editable blockchain for block validation, the advantages of which become more significant as the scale of data collection grows [22]. Cheng, J.C.P. et al. proposed a novel framework based on blockchain and cryptography to maintain data accountability and confidentiality in engineering cost management [23].

3. Design of Blockchain-Based Traceability Model for Taishan Tea

3.1. Design Ideas

Taishan tea products are divided into green tea, black tea, yellow tea, and other varieties. The production process is complex, including planting, picking, processing, warehousing, and the sales of five major links. Among them, the processing link is more complicated, and different tea species need to use specific processing technology; the link in the acceptance of raw materials, acceptance of auxiliary materials, killing, drying, fermentation, kneading, drying, and so on, for the quality and safety of the key points, as well as the need for enterprise control and government supervision. Aiming at the whole industry chain of Taishan tea products and the key points of quality and safety in each link, the design of the Taishan tea product quality and safety credible traceability model can not only realize the whole process of quality and safety traceability of Taishan tea products but also ensure the authenticity and credibility of the traceability data.

In order to achieve a high degree of transparency of information and enhance the trust of all parties involved in the Taishan tea industry chain, we propose a blockchain-based Taishan tea traceability model that ensures that all parties in the Taishan tea industry chain can trace the relevant information. Our goal is to realize the traceability of the entire Taishan tea industry chain and enhance the trust and transparency associated with it. In order to ensure the quality and safety of the entire Taishan tea industry chain, we designed a credible traceability model for Taishan tea product quality and safety, which can both track the quality and safety of the entire Taishan tea production process and ensure the authenticity and credibility of the recorded traceability data.

(1) Integration of blockchain and traceability systems

Blockchain technology is applied to solve the problems of the traditional Taishan tea product traceability system, such as centralized management and low data credibility. Blockchain technology can improve the transparency and security of data and ensure the reliability and non-tampering of Taishan tea product quality and safety information. The data types involved in Taishan tea products are shown in Figure 1, which divides the data, in which part of the planting information data, the administrator data of each link, and so on, are non-uplinked data, and the planting, picking, warehousing, processing, and logistics data of each link are uplinked data. Combined with the design idea of "one link, one ledger", separate ledgers are set up for each link's traceability data to store key traceability data. This design not only reduces the amount of data uploaded by the traceability system but also greatly alleviates the efficiency problems caused by uploading a large amount of system data.

Through visits and research in Taishan tea enterprises and communication with Taishan tea consumers, we accurately identify and determine a series of key factors affecting the quality of Taishan tea. For the Taishan tea industry chain, we accurately collected these key data with the help of IoT devices. These data are then carefully categorized into two main categories: uplinked data and non-uplinked data. The on-chain data refers to the information encrypted by blockchain technology and stored in the distributed ledger, which is crucial to ensure the authenticity and tampering of Taishan tea traceability, while the off-chain data may contain some auxiliary information that does not have high real-time requirements or requires specific processing before considering whether or not to be on-chained. Such categorization not only improves data processing efficiency but also enhances the flexibility and practicality of the traceability system.

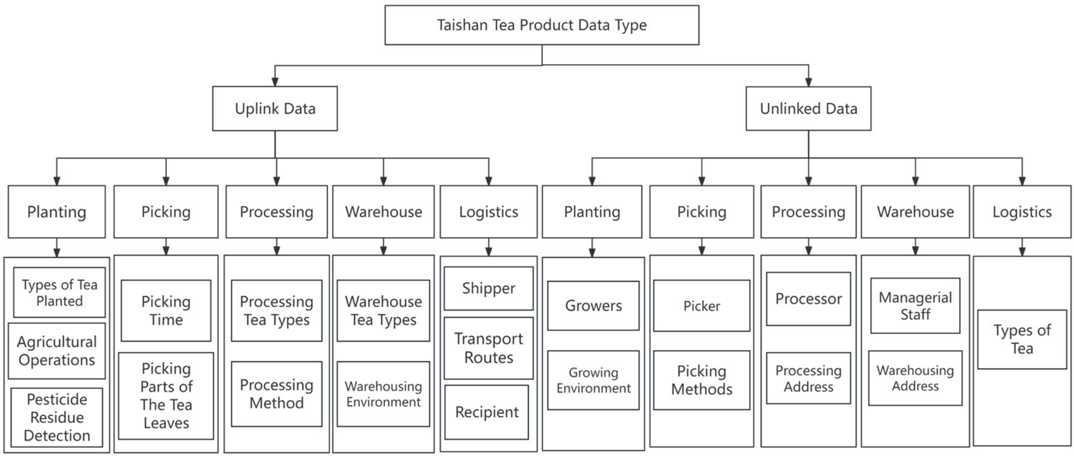

Figure 1. Taishan tea product data type.

(2) Embedding the SM2 optimization algorithm

The SM2 encryption algorithm is an asymmetric encryption algorithm based on elliptic curve cryptography (ECC), which contains functions such as digital signature, key exchange, and public key encryption and has the advantages of high cryptographic complexity, fast processing speed, and smaller machine performance consumption. The algorithm is based on the elliptic curve discrete logarithm problem and is mainly used in cryptography fields such as digital signature, key exchange, encryption, etc. Feng, M.Q. et al. demonstrated the unforgeability and anonymity of the scheme by converting SM2 digital signatures to Type-T and integrating DualRing with a variant of SM2 digital signatures and proposed an optimized linkable scheme [24]. Hu, J.H. et al. improved the efficiency of signature and verification of SM2 algorithms by optimizing part of the SM2 signature algorithms with inverse operations during the process and improved the efficiency of signature and verification of SM2 algorithms by reducing the inverse operation during the whole process, effectively reducing time complexity and improving the signature and verification efficiency of the SM2 algorithm [25]. The successful release and implementation of the SM2 algorithm reflects China's technological advancement in the field of cryptography and its important contribution to information security.

Data storage in the blockchain system is characterized by openness and transparency; however, there is a large amount of data such as the core processing technology of enterprises in the processing and production process of Taishan tea products, which should not be disclosed to the public. To address this problem, the SM2 encryption algorithm is utilized to encrypt the core confidential data that needs to be uploaded to the blockchain, and then the uplink operation is carried out. First, the Taishan tea production process of each company is investigated to determine the steps of the link that need to be encrypted and stored. For example, Taishan tea products planting tea species, agricultural operations, pesticide residue testing, picking time, and so on are confidential processing data of the enterprise, combined with the SM2 algorithm and blockchain technology, in the superledger of the processing link; this kind of data is stored in the ciphertext. In order to prevent the data from being intercepted or maliciously altered during data transmission in the system, the more secure SM2 algorithm is utilized to encrypt the confidential data for transmission, which provides a guarantee for the security of data storage and transmission.

(3) Hierarchical up-linking mechanism

The core of our research focuses on the strategy of grading and managing key information in the production process of Taishan tea. In view of the huge amount of data generated in the cultivation and production process of Taishan tea, we particularly focus on those key information points that directly affect the quality of tea and plan to utilize blockchain technology to realize the on-chain storage of these key information to ensure the security and tampering of their data.

When constructing the blockchain-based Taishan tea traceability model, we fully recognize the complexity of concurrent use by multiple enterprises. Under this model, each production link is considered equally important and indispensable; therefore, we do not present a fixed information grading system. Instead, we strive to ensure that all participating companies can share and trace the whole process of Taishan tea information in an efficient and transparent way through a refined data processing strategy, so as to jointly promote the quality and brand value of Taishan tea.

In view of the peak load problem that may occur in the actual production process of Taishan tea products, we pay special attention to the performance of the alliance chain network in the face of a large number of uplink requests. Due to the limitation of the transaction speed of the alliance network, the short-term surge in transaction volume may lead to network blocking, which, in turn, affects the normal uploading of data and destroys the consistency and integrity of data.

To effectively deal with this challenge, this paper innovatively proposes a hierarchical uploading mechanism. This mechanism aims to dynamically grade the data to be uploaded according to the importance and urgency of the data. By rationally deploying resources and prioritizing critical and urgent data, we can effectively avoid the blocking phenomenon of the alliance chain network while guaranteeing the timeliness and accuracy of data and ensuring the integrity and traceability of Taishan tea production data. The implementation of this mechanism will further enhance the reliability and practicability of the Taishan tea traceability model and provide strong support for the sustainable development of the Taishan tea industry.

In our in-depth communication with Taishan tea enterprises, we have accurately identified and determined a series of key factors affecting the excellent quality of Taishan tea. In order to ensure the integrity, authenticity, and security of these valuable data, we adopt blockchain technology to collect these key factors directly through IoT devices, and, after strict screening and processing, securely upload and store them. This process not only guarantees the traceability of the data but also builds a solid digital cornerstone for the quality regulation and consumer trust of Taishan tea. We have mapped these in Table 1.

The sources of non-uplinked data are wide and varied, and they may originate from the collection of IoT devices, or from the registration of information in the internal management system of the enterprise, which are mainly supplementary to the traceability information of Taishan tea and participate in the daily operation and decision-making of the enterprise; moreover, they are not directly involved in the key influencing factors that determine the quality and inferiority of Taishan tea. We plotted these data in Table 2.

Table 1. Uplink data type.

	Industrial Chain Link	**Data Example**
Uplink Data	Planting	Types of Tea Planted Agricultural Operations Pesticide Residue Detection
	Picking	Picking Time Picking Parts of The Tea Leaves
	Processing	Processing Tea Types Processing Method
	Warehouse	Tea Types Environment
	Logistics	Shipper Transportation Routes Recipient

Table 2. Unlinked data type.

Unlinked Data	Planting	Growers Growing Environment
	Picking	Picker Picking Methods
	Processing	Processor Processing Address
	Warehouse	Managerial Staff Warehousing Address
	Logistics	Types of Tea

In order to improve the efficiency of Taishan tea data uploading and prevent network congestion, we plan to implement a data hierarchy strategy that prioritizes critical data that have a significant impact on tea quality, followed by the rest of the data. This strategy aims to ensure that critical information is recorded and shared instantly while reducing network pressure due to data deluge. Given the huge amount of data generated during the cultivation and production of Taishan tea, we focus on those data points that have a decisive impact on the quality of tea and propose to use blockchain technology to ensure that this critical information is tamper-proof and highly secure. In building a blockchain-based Taishan tea traceability model, we need to flexibly cope with the complex environment of concurrent use by using multiple enterprises, treating each production link as equally important and not presetting a fixed hierarchy of information grading. Instead, we will promote efficient and transparent sharing and tracing of the whole process of Taishan tea information among all participating enterprises through a refined data processing mechanism, so as to jointly guard and enhance the quality and brand value of Taishan tea.

Through in-depth communication with Taishan tea enterprises, consumers, and sellers, we systematically integrated multi-dimensional information about the quality of Taishan tea and accurately extracted the core elements and secondary factors that determine its quality. Core factors, as the first and most critical data indicators affecting the quality of Taishan tea, were established as the first object of analysis. As for the secondary factors, although their influence on the quality is slightly less, they are equally important, and we have refined them into primary and secondary data and implemented a differentiated upward chaining strategy. This strategy aims to significantly improve the efficiency and accuracy of data processing through refined classification and an efficient uploading process, so as to grasp the quality characteristics of Taishan tea in a more comprehensive and precise manner. We plotted these data in Table 3.

Table 3. Uplink data classification.

Industrial Chain Link	Data Classification	Data Example
Planting	Level 1	Pesticide Residue Detection
	Level 2	Types of Tea Planted Agricultural Operations
Picking	Level 1	Picking Time
	Level 2	Picking Parts of The Tea Leaves
Processing	Level 1	Processing Method
	Level 2	Processing Tea Types
Warehouse	Level 1	Environment
	Level 2	Tea Types
Logistics	Level 1	Shipper Recipient
	Level 2	Transportation Routes

When the data upload request is made, the priority of the uploaded data is detected, and its hash value is taken to pack the data of the same level for processing, and the packaged data are P = [A_1, A_2 ... A_n], in which A_n is a complete Taishan tea product data, and n denotes the granularity of the data packing, and each time the packages are packed in batches with n data as the basic unit. The packaged data are uploaded into the blockchain network to ensure the integrity of the data, and, at the same time, serialize the data packet and take its hash value. The blockchain detects the hash value belonging to the first-level data and prioritizes the uploading of such data.

3.2. Blockchain-Based Taishan Tea Traceability Process

According to the above design ideas, on the basis of the traditional Taishan tea traceability model, combined with the process of the Taishan tea industry chain, the traditional centralized traceability system is reconstructed; based on the design idea of "one link, one ledger", the traceability data that need to be uploaded to the chain in each link are stored in separate ledgers, so as to establish a new distributed traceability system architecture.

After extensive research on a number of representative enterprises, in-depth research on the Taishan tea industry, and field visits to related enterprises, we have systematically sorted out the complete process of Taishan tea from cultivation to production and elaborately drew a flowchart that comprehensively covers the complete process of Taishan tea from cultivation to processing. The flow chart summarizes the core operation steps of each key link and promotes a comprehensive understanding of the culture and industrial value of Taishan tea. The above is shown in Figure 2.

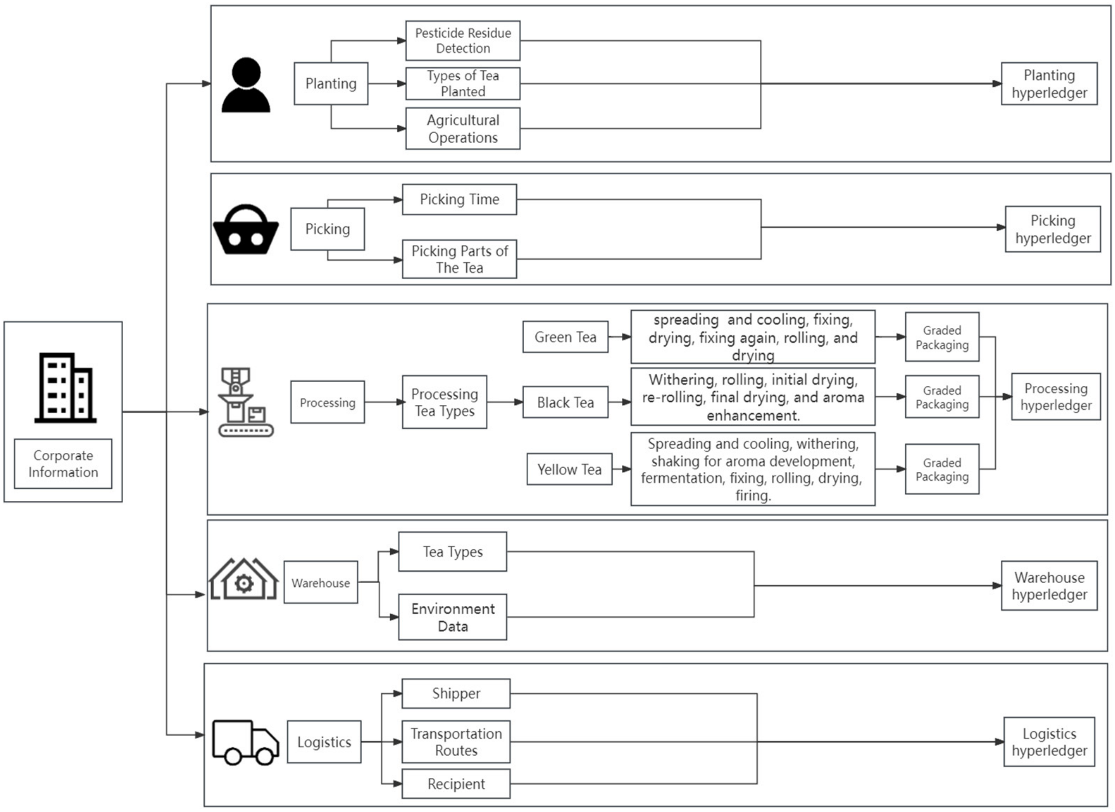

Figure 2. Taishan tea traceability process.

The traceability process is summarized below:

(1) According to the traceability process of Taishan tea products, we divide it into five major links: planting, picking, processing, storage, and logistics. In each link, the steps involving the quality of Taishan tea products are regarded as the key factors affecting the quality of Taishan tea and need to be operated on the chain. This ensures that the entire production process of Taishan tea products is traceable, thus improving product quality and consumer trust.

(2) The planting link covers all the farming operations in the process of Taishan tea planting. During the planting process and before the harvesting of Taishan tea, agricultural products will be tested to ensure that Taishan tea meets safety and quality standards. The test results will be recorded and stored in the superledger of the planting process together with the data of agricultural operations, so as to facilitate subsequent inquiries and traceability.

(3) Picking time has a profound impact on Taishan tea, which not only determines the quality characteristics such as tenderness, taste, aroma, and color but also directly relates to the yield and economic benefits of tea. In Taishan tea picking, the careful selection of buds and leaves is crucial, following the high standard of "one bud, one leaf", and picking at the best time in the spring to ensure the tenderness and uniformity of the tea, and thus enhance the overall quality of tea and market competitiveness.

(4) Different types of Taishan tea require different processing methods due to their unique characteristics and flavors. The processing of each type of Taishan tea requires precise control of temperature, humidity, time, and other key parameters to ensure the quality of the final product. If there are missing steps in the processing process or if the processing method is not in place, the quality of the Thai tea leaves will be affected. The information generated from the processing needs to be uplinked and processed to ensure the quality and safety of Thai tea.

(5) The warehousing link includes storage of tea species and environmental data. Tarzan tea is prone to a series of quality and safety problems in the storage link; therefore, the storage environment data of Tarzan tea are sensitive data of quality and safety. Consumers and enterprises can view the environmental data of the warehouse in real time, and consumers can also visually view the storage environment to improve the credibility of the product quality and safety, and, ultimately, the environmental data will be stored in the superledger of the storage link.

(6) The logistics link includes data on the shipper, the transportation route of Taishan tea, and the receiver. These data not only track the physical location of the goods, but also provide important information for managing, monitoring, and optimizing the supply chain, providing strong support for decision-making.

(7) Finally, we organize and analyze the information generated from the five major links of planting, picking, processing, warehousing, and logistics, and design a comprehensive Taishan tea traceability model. In this model, non-uplinked data involved will be stored in a centralized database, which can effectively reduce the efficiency pressure of the blockchain and improve the performance of the overall system.

4. Analysis of Blockchain-Based Taishan Tea Traceability Model

4.1. Blockchain-Based Taishan Tea Traceability Model Architecture

In the planting stage and picking stage, Taishan tea planting presents a small-scale nature of multiple growers, which makes it difficult to deploy a unified IoT cluster and requires the targeted selection of suitable IoT devices for data collection. In the processing, warehousing, and logistics links, the production mode of Taishan tea is relatively fixed and large-scale, which supports the large-scale deployment of IoT clusters and the automatic sensing and collection of basic information. The whole industry chain of agricultural products is characterized by many nodes of participating subjects, a long industry chain, a wide range, a large amount of data, and multiple sources of heterogeneity; therefore, the principle of hierarchical data uploading is adopted to alleviate the pressure of the blockchain network.

We have thoughtfully designed the architecture diagram of the Taishan tea traceability system, which is conceived based on our in-depth dialog with Taishan tea enterprises and extensive study of Taishan tea-related information. This architecture diagram adopts the form of a flowchart, which intuitively and clearly shows the complete chain from data collection driven by IoT technology to data refinement processing until the final application. At each key node of the Taishan tea industry chain, IoT equipment operates efficiently, accurately capturing and aggregating core data. Subsequently, these data undergo a series of rigorous data processing processes to ensure the accuracy, integrity, and security of the data, providing impenetrable technical support and data protection for the full traceability of Taishan tea products. The above is shown in Figure 3.

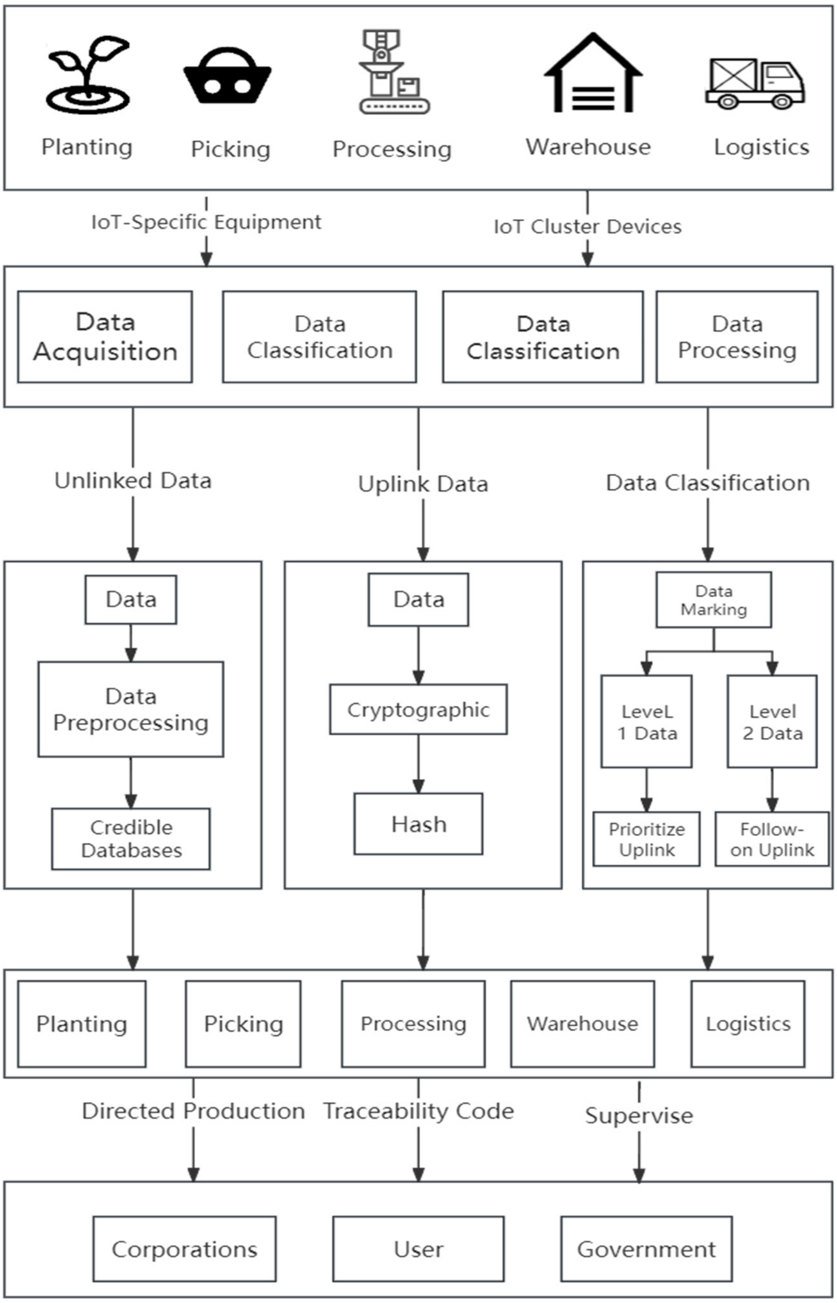

Figure 3. Taishan tea traceability construct.

4.2. SM2 Encryption Algorithm Optimization

The combination of blockchain and SM2 asymmetric encryption algorithm will inevitably affect the performance of model transmission and storage; in order to solve this problem, the encryption and decryption algorithm of SM2 is analyzed in detail, the characteristics of the key derived function character splicing is used as an entry point, and concurrent processing is utilized to optimize the efficiency of the SM2 algorithm and thus the performance of the traceability system.

4.2.1. Optimization of SM2 Algorithm Based on Concurrent Processing

Data encryption plays a decisive role in the security of data, and the performance of encryption algorithms directly affects the performance of data storage and transmission. In SM2 encryption algorithm, the key derivation function needs to utilize bit string and cryptographic hash algorithm to generate the key data bit string, and its algorithm flow is shown in Figure 4 (where Hai denotes the hash value, ct denotes the counter, klen denotes the length of the key, v denotes the step value, and K denotes the final secret key). In the traditional key derivation function, it is necessary to perform a number of subtasks, and the number of subtasks is determined by the length of the key data bits that need to be obtained and the length of the hash value data output by the cryptographic hash algorithm. In the subtasks, the bit string is used to execute the cryptographic hash algorithm by splicing different parameters as inputs, and, finally, the key data bit string is obtained according to splicing the results of multiple subtasks. It can be found that during the execution of the key derivation function, the execution of the bit string in the cryptographic hash algorithm is independent of each other until all the subtasks are executed, and the final result is obtained by splicing the execution results. Based on the above, we draw a flowchart of the operation mechanism of the traditional SM2 encryption algorithm, as shown in Figure 4.

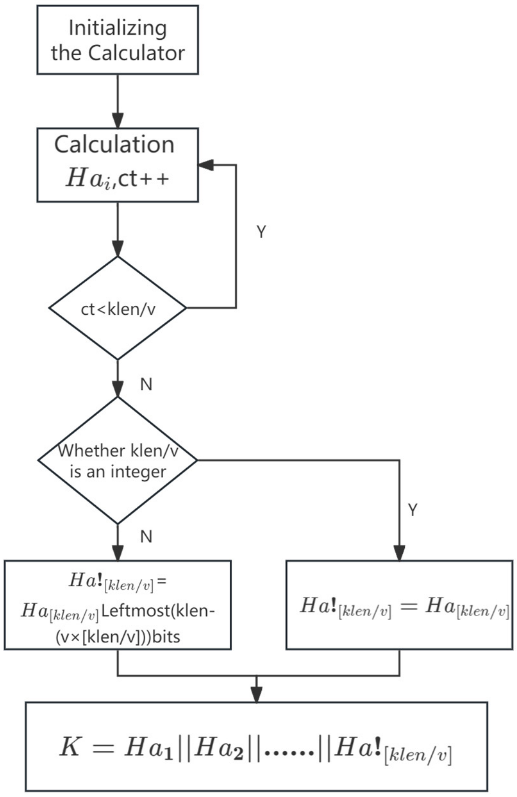
Initializing the Calculator
Calculation Ha_i,ct++
Y
ct<klen/v
N
Whether klen/v is an integer
Y
N
$Ha!_{[klen/v]}$= $Ha_{[klen/v]}$Leftmost(klen-(v×[klen/v]))bits
$Ha!_{[klen/v]} = Ha_{[klen/v]}$
$K = Ha_1||Ha_2||......||Ha!_{[klen/v]}$

Figure 4. Flow chart of key derivation function.

Based on the above process description, the execution efficiency of the key derivation function depends on the number of subtasks and the execution efficiency of the cryptographic hash algorithm, while, in the actual application process, the length of the bit string is often long, resulting in a large number of subtasks, and the execution efficiency of the cryptographic hash algorithm is difficult to be effectively improved, resulting in the inefficiency of the SM2 cryptography algorithm for encrypting long text.

Therefore, this paper proposes an optimization method of SM2 encryption algorithm based on a concurrent processing framework, which combines the process of key derivation function generating key data bit string using bit string and cryptographic hash algorithm with the concurrent processing framework and performs concurrent processing for the process of executing cryptographic hash algorithm on the sub-string, which eliminates the waiting time for the process of executing cryptographic hash algorithm many times during the execution of a single process. The algorithmic flow is shown in Figure 5. Based on the above, we constructed a flowchart of the operation mechanism of the improved SM2 encryption algorithm.

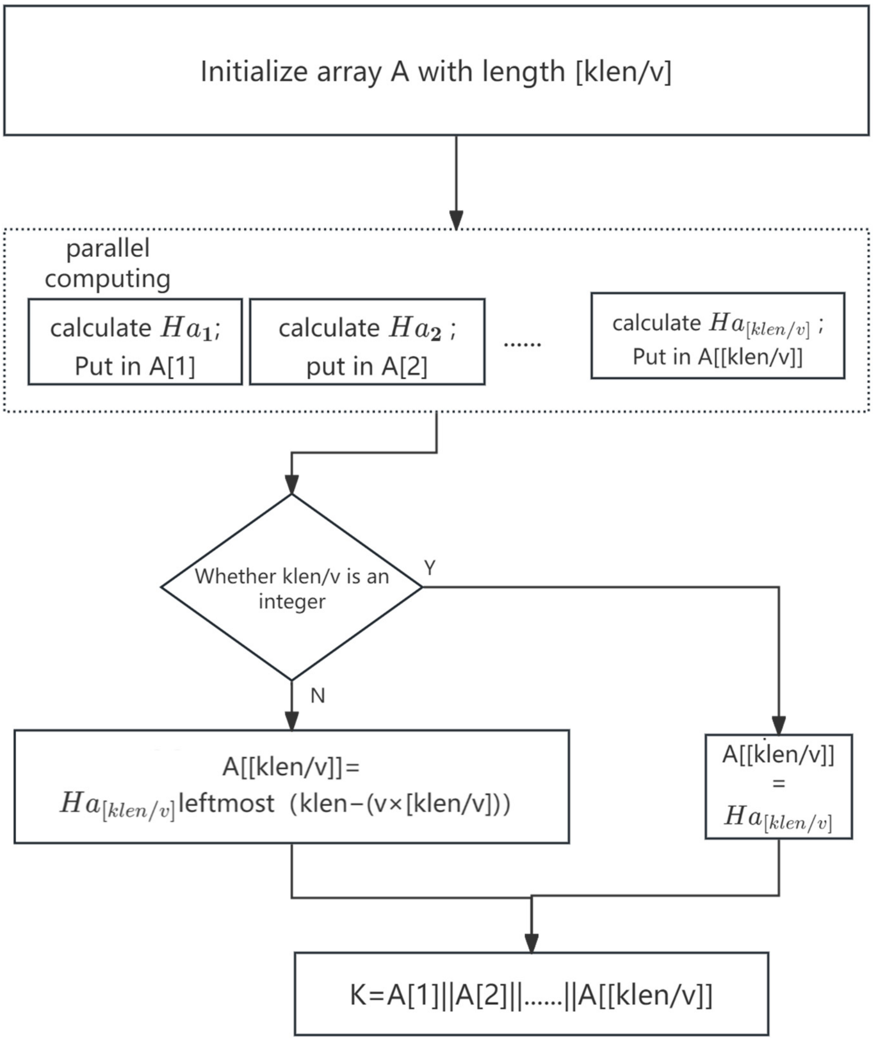
Initialize array A with length [klen/v]
parallel computing
calculate Ha_1; Put in A[1]
calculate Ha_2 ; put in A[2]
......
calculate $Ha_{[klen/v]}$; Put in A[[klen/v]]
Whether klen/v is an integer
Y
N
A[[klen/v]]= $Ha_{[klen/v]}$leftmost (klen−(v×[klen/v]))
A[[klen/v]] = $Ha_{[klen/v]}$
K=A[1]||A[2]||......||A[[klen/v]]

Figure 5. Flow chart of revised key derivation function.

The subtasks of the key derivation function are decomposed into multiple independent computational units (subtasks). These subtasks can be processed concurrently, avoiding the time delay caused by serial execution. By introducing a concurrent processing framework, multiple subtasks can be executed concurrently in different computational processes. Specifically, the optimized algorithm, after splicing the parameters required for subtasks, assigns these tasks to multiple computational processes at the same time so that each process executes the hash algorithm independently. Under the concurrency framework, the hash operations of subtasks can be performed simultaneously and are no longer executed sequentially. For example, if there are n subtasks and the system supports m concurrent processes, the execution time will be reduced from the original O(n) to O(n/m). This significantly improves the efficiency of encryption execution. After all subtasks are completed, the output of each sub-task is spliced to generate the final key bit string and complete the encryption process.

Under the concurrent processing framework, utilizing the multi-process characteristic of computers, the execution process of multiple subtasks in the cryptographic hash algorithm is carried out concurrently; after the splicing of the parameters required by multiple subtasks is completed, the concurrent processing framework runs multiple cryptographic hash algorithms in multiple processes in the system. If the number of subtasks is n, the maximum number of concurrent processes supported by the system is m, the execution time of a single cryptographic hash algorithm is t: when n is small, the execution time of the key derivation function is close to t; when the number of substrings is large, the substrings are processed in batches, and the execution time of the key derivation function is close to t × n/m.

The optimized SM2 algorithm successfully reduces the time complexity from O(n) to O(n/m) by introducing a concurrent processing framework, where n is the number of subtasks and m is the number of concurrent processes. This optimization greatly reduces the waiting time during the encryption process, especially when dealing with large-scale data or facing highly concurrent requests, such as the simultaneous submission of data by multiple users in a blockchain system, and the algorithm shows more stable and efficient performance. The optimization not only improves the encryption speed but also significantly reduces the latency of the encryption and decryption processes, ensuring that the system can quickly respond to large-scale data processing needs, especially for data-intensive and high-frequency transaction scenarios.

4.2.2. Algorithm Performance Testing

The SM2 encryption algorithm is a deterministic algorithm, and the output of the algorithm is deterministic without any random factors or uncertainty, ensuring the consistency and stability of the output given the same input, excluding random factors and uncertainty, and no error or fluctuation, thus becoming an indispensable key in encryption and data integrity verification, further consolidating the basis of its application in the security field.

Regarding the algorithm performance test of the SM2 algorithm based on concurrent processing, the design experimental data were as follows: 10,000 characters, 15,000 characters, 20,000 characters, 25,000 characters, 30,000 characters, 35,000 characters, 40,000 characters, 45,000 characters, and 50,000 characters, according to the different lengths of the text. The performance of the KDF function, SM2 encryption algorithm, SM2 decryption algorithm in the encryption, and decryption process are tested to obtain the performance of the algorithms before and after the optimization. On the basis of the above experiments, we obtained the corresponding experimental results about the performance comparison graph between the traditional SM2 encryption algorithm and the improved SM2 encryption algorithm. The experimental results are shown in the following figure. Among them, Figure 6 is a time consumption comparison chart of the KDF function in the encryption process. Figure 7 is a time consumption comparison chart of the KDF function in the decryption process. Figure 8 is a SM2 encryption algorithm optimization comparison chart. Figure 9 is a SM2 decryption algorithm optimization comparison chart.

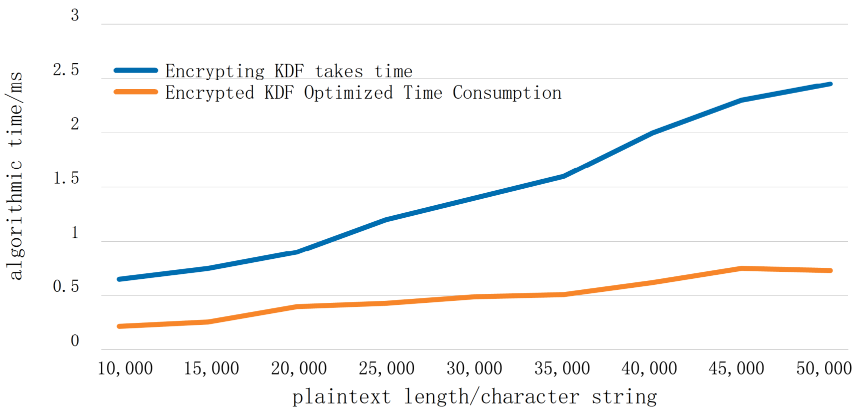

Figure 6. Time consumption comparison chart of KDF function in the encryption process.

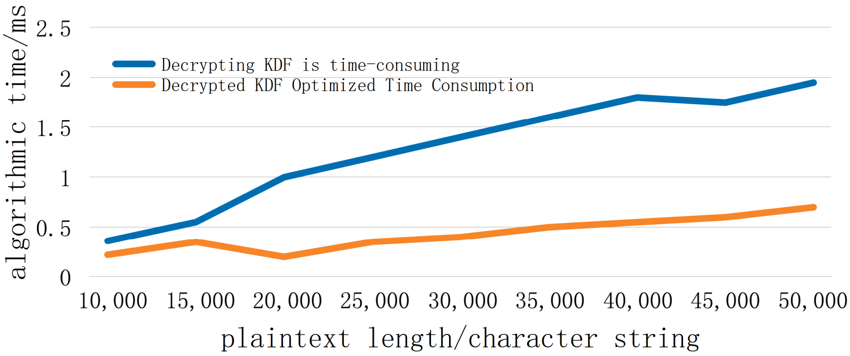

Figure 7. Time consumption comparison chart of KDF function in the decryption process.

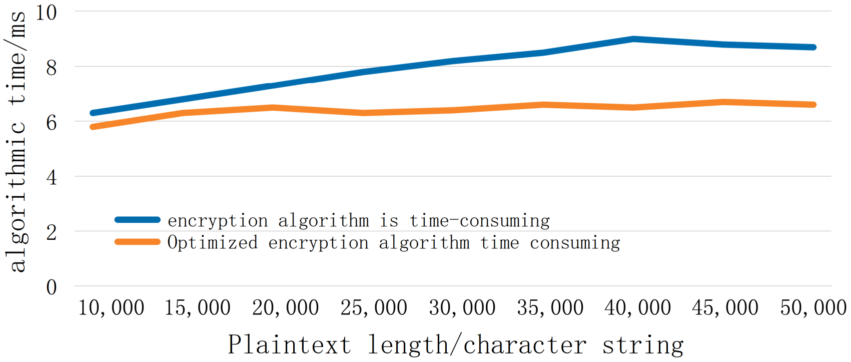

Figure 8. SM2 encryption algorithm optimization comparison chart.

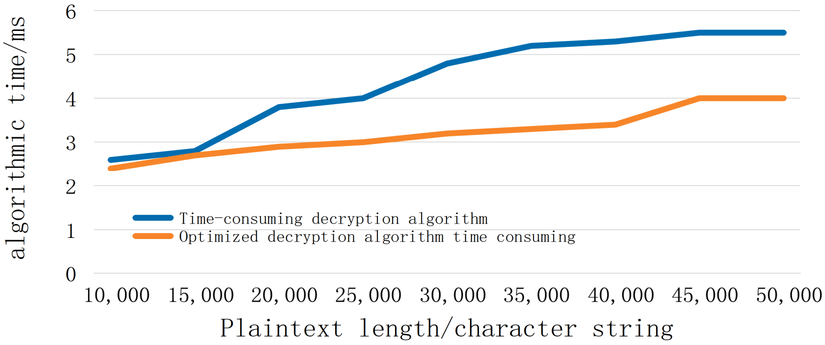

Figure 9. SM2 decryption algorithm optimization comparison chart.

According to the line graph, it can be found that, for plaintext data with long text, the time consumed by the KDF function after concurrent processing is significantly reduced, and as the length of the text increases; the improvement of the overall performance of the encryption and decryption algorithms of SM2 also increases. It can be seen that the combination of the concurrent processing framework and key derivation function significantly improved the efficiency of SM2's encryption and decryption algorithm.

In large-scale data processing systems such as blockchain, even a 1% efficiency improvement will have an extremely significant effect when accumulated over thousands of cryptographic operations. A tiny reduction in time for a single operation can dramatically reduce overall processing time at the system level, and this optimization is critical to improving overall system performance. Users often notice these subtle improvements in performance, especially in time-sensitive applications, where reduced latency translates directly into a smoother and faster user experience. As the data volume expands and the user base increases, small initial optimization measures will show significant performance advantages in the future when facing larger-scale applications, laying a solid foundation for long-term scalability and the efficient operation of the system.

4.3. Data Hierarchical Transmission Strategy

When an enterprise uploads data, it divides the key information into uplinked data and non-uplinked data, in which the uplinked data are divided into two levels, i.e., level 1 data and level 2 data, and the uplinked data are referred to as CH-D_i, level 1 data are referred to as CH-D_1, and level 2 data are referred to as CH-D_2 for ease of description. When the data are uploaded, priority is given to selecting the level 1 data to be uplinked. Pack the level 1 data of each link as P. Each data packet P contains n pieces of data. Then, we construct these n pieces of data into a Merkle tree.

First, each datum is computed by the SHA256 hash function to obtain N leaf nodes, where Node_i has the value of SHA256 (CH-D_i). Secondly, the neighbor nodes Node_1 and Node_2, their parent nodes $\mathrm{Node}_{[1,2]}$, and the value of $\mathrm{Node}_{[1,2]}$ is $\mathrm{Hash}_{[1,2]}$ = SHA256($\mathrm{Hash}_1 \mid\mid \mathrm{Hash}_2$). According to the above method, $\mathrm{Node}_{[3,4]}$, $\mathrm{Node}_{[5,6]}$, etc., are continuously generated. Next, for the leading nodes $\mathrm{Node}_{[1,2]}$ and $\mathrm{Node}_{[3,4]}$, their parent node $\mathrm{Node}_{[1,4]}$ is generated upwards, and the value of node $\mathrm{Node}_{[1,4]}$ is $\mathrm{Hash}_{[1,4]}$ = SHA256($\mathrm{Node}_{[1,2]} \mid\mid \mathrm{Node}_{[3,4]}$). According to the above method, keep generating Node until $\mathrm{Node}_{[i,i-3]}$. Finally, the N leaf nodes are synthesized into a root node.

After the first-level data transmission of each planting and production link is completed, the second-level data of the link will be transmitted, which can ensure the completeness and accuracy of the data, and, at the same time, avoid confusion and errors in the data transmission process, as well as avoid data blocking.

5. Performance Test of Blockchain-Based Taishan Tea Traceability Model

5.1. Experimental Analysis

In order to comprehensively assess the performance difference in data processing between the blockchain-based Taishan tea traceability model and the traditional Taishan tea traceability model, we encapsulated both of them into standardized API interfaces and executed exhaustive performance tests using Postman (v11.1.14.0), an interface testing tool. The tests cover three aspects: data writing (simulating concurrent submission of tea production information by multiple users), data querying (testing response time and accuracy under different query conditions), and throughput (evaluating the system's overall processing capability under high pressure). Through comparative analysis, the results in the response are verified to match the expected results. The experimental environment is based on an i9-12900K CPU (Intel, Santa Clara, CA, USA), a Centos7.9 operating system, and version 1.4.6 Fabric for testing.

5.2. Model Performance Testing

5.2.1. Data Write and Data Query

System response time, i.e., the response time of the system to user requests or inputs, is a key indicator of system performance and user experience. It covers the whole process from the time the request is sent to the blockchain network until the result is obtained, which is directly related to the availability of the system and the speed of transaction confirmation, and a shorter response time usually signifies higher system performance and faster operational efficiency. We conducted 50 rounds of tests on the blockchain-based Taishan tea traceability model and the traditional Taishan tea traceability model, respectively, with 2000 sets of data in each round. Based on the above experiments, we obtained the corresponding experimental results, which are shown in the following figures, where Figure 10 represents the comparison of query time and Figure 11 represents the comparison of write time.

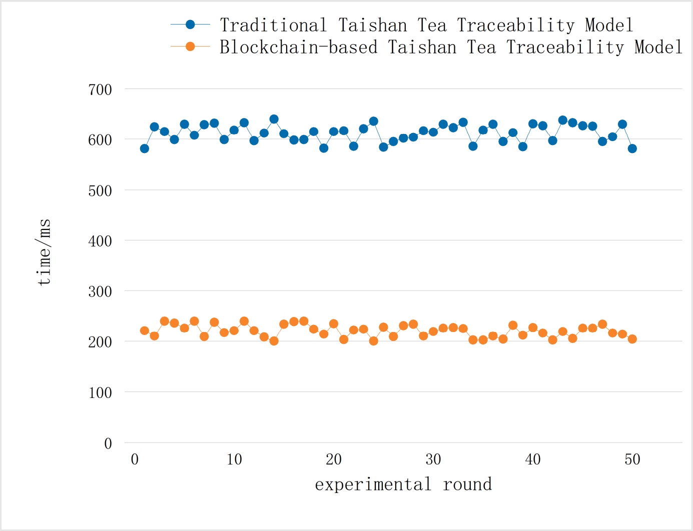

Figure 10. Inquiry time comparison chart.

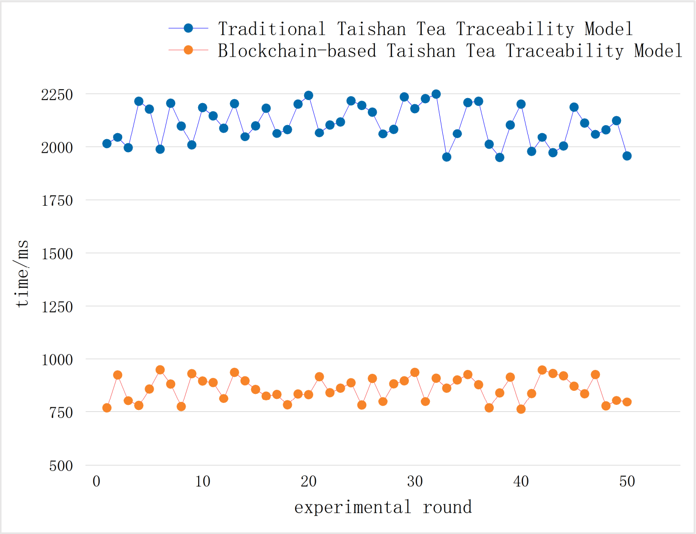

Figure 11. Write query comparison chart.

From the test results, it can be seen that the test performance of the blockchain-based Taishan tea traceability model is stronger than that of the traditional Taishan tea traceability model in both data query and data writing. The test results show that the performance of the blockchain-based Taishan tea traceability model is stronger than the traditional Taishan tea traceability model in terms of data query and data writing.

5.2.2. Throughput Testing

Throughput is generally expressed as transactions per second (TPS), which is the number of things processed per second transmitted, and the system will have a processing time after receiving a task. In this test, we prepared four datasets with 1000, 3000, 5000, and 7000 pieces of data, and each dataset was tested for 30 rounds. Based on the above experiments, we obtained the corresponding experimental results, which are shown in the following figures, where Figure 12 is 1000 TPS, Figure 13 is 3000 TPS, Figure 14 is 5000 TPS, and Figure 15 is 7000 TPS.

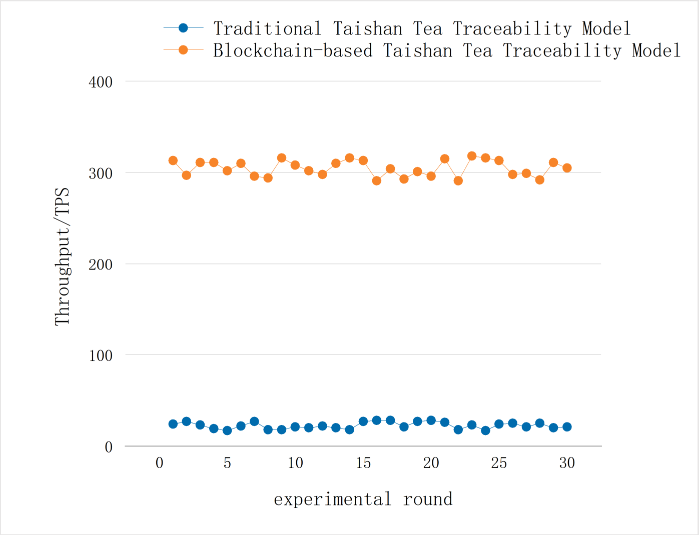

Figure 12. One thousand TPS.

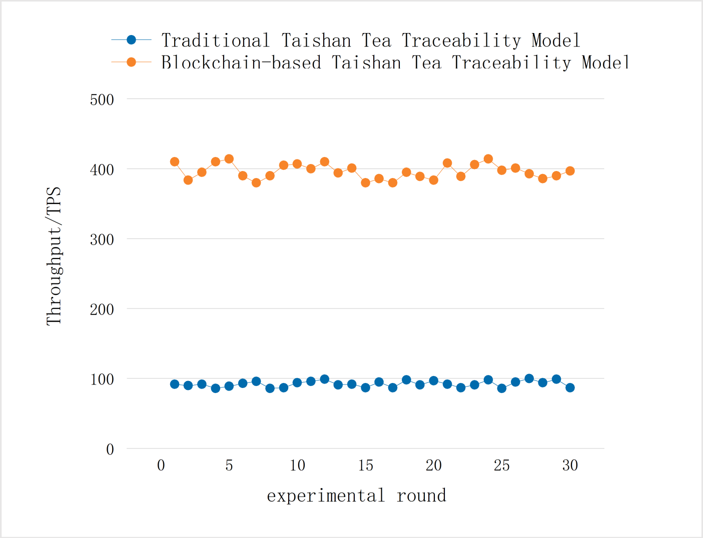

Figure 13. Three thousand TPS.

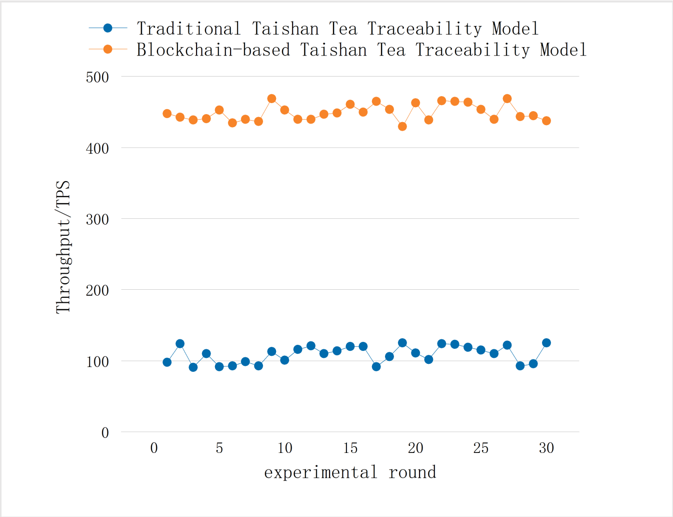

Figure 14. Five thousand TPS.

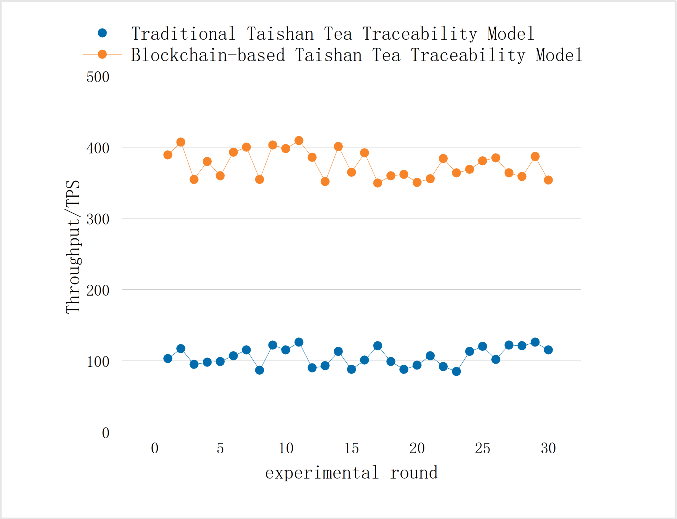

Figure 15. Seven thousand TPS.

5.3. Analysis of Test Results

In the data query and data writing test phase, the blockchain-based Taishan tea traceability model performs better than the traditional Taishan tea traceability model. In the throughput test phase, when the transaction volume is less than 5000, the blockchain-based Taishan tea traceability model has a larger throughput and a more stable performance; when the transaction volume is more than 5000, both models fluctuate, but the throughput of the blockchain-based Taishan tea traceability model still outperforms the traditional Taishan tea traceability model. The experimental results show that the blockchain-based Taishan tea traceability model has a greater improvement compared with the traditional Taishan tea traceability model.

6. Discussion

6.1. Summaries

With the improvement in people's requirements for tea quality, the food safety of Taishan tea is becoming more and more important. For this reason, this paper applies blockchain technology to the traceability of Taishan tea products, which is used to solve the problems of low efficiency and low credibility of traditional Taishan tea traceability. On the basis of the Taishan tea traceability standard document, the characteristics of each basic data item are analyzed, and the blockchain-based Taishan tea traceability model is designed. In this paper, the blockchain-based Taishan tea traceability model was tested for its performance, and the results feedback that the scheme of this paper is sufficient in practice to meet the daily needs of various stages of Taishan tea food processing and production, and can realize the effective uploading, controllable supervision and credible traceability of Taishan tea product information, which can provide certain guarantee for the healthy and sustainable development of the Taishan tea industry chain.

(1) According to the Taishan tea planting and production process, combined with the actual Taishan tea production, the blockchain-based Taishan tea traceability model is constructed, which effectively solves the problems of data opacity and poor data credibility in the traditional Taishan tea traceability model, and, at the same time, divides the data into uploaded data and non-uploaded data, which improves the efficiency of data uploading.

The improvement in data query and write speed means that blockchain-based traceability models can process more data requests in the same amount of time, thereby improving the overall efficiency of the traceability system. The test results show that in the experiments of data querying and data writing, our blockchain-based Taishan tea traceability model outperforms the traditional Taishan tea traceability model in terms of data querying speed and data writing speed; moreover, our blockchain-based Taishan tea traceability model outperforms the traditional Taishan tea traceability model in terms of throughput in the case of high transaction volume.

(2) The optimization of the SM2 algorithm further improves the efficiency of the blockchain-based Taishan tea traceability model. In this paper, the blockchain-based Taishan tea traceability model was pressure tested, and the results feedback that the scheme in this paper can meet the daily needs of the actual stage of Taishan tea food processing and production to a certain extent, and can realize the effective uploading, controllable supervision, and credible traceability of Taishan tea product information, which can provide a certain guarantee for the healthy and sustainable development of the Taishan tea industry chain.

6.2. Prospects

(1) We can design IoT smart devices to collect data from all aspects of the product from planting to sales, and automatically upload these data to the blockchain network to ensure the authenticity and non-tamperability of the data, the efficiency and accuracy of data collection, and the automatic uploading of these data to the blockchain network, which not only dramatically improves the efficiency of data collection and reduces the number of manual entry errors and delays but also ensures the authenticity and non-tamperability of the data.

(2) With the continuous maturity of the technology and the deepening of the modularized design, the traceability model for agricultural products will be able to adapt more flexibly to the needs of diversified agricultural products and their complex and changing supply chains. Different types of agricultural products will be able to realize full and transparent traceability with the help of this technology, providing consumers with safer and more reliable food security. At the same time, the application of blockchain technology will further consolidate the security and transparency of the data and meet the high standards of data protection required by various industries.

Author Contributions: Conceptualization, K.L. and P.L.; methodology, K.L. and P.L.; validation, K.L. and P.L.; investigation, S.G., K.L. and P.L.; writing—original draft preparation, K.L.; writing—review and editing, P.L.; visualization, K.L. and P.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, and further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Miao, S.W.; Wei, Y.; Pan, Y.; Wang, Y.F.; Wei, X.L. Detection methods, migration patterns, and health effects of pesticide residues in tea. *Compr. Rev. Food Sci. Food Saf.* **2023**, *22*, 2945–2976. [CrossRef]
2. Rao, S.H.; Chen, F.Q.; Hu, W.; Gao, F.; Huang, J.K.; Yi, H.M. Consumers' valuations of tea traceability and certification: Evidence from a blockchain knowledge experiment in six megacities of China. *Food Control* **2023**, *151*, 109827. [CrossRef]
3. Wei, Y.; Wen, Y.Q.; Huang, X.L.; Ma, P.H.; Wang, L.; Pan, Y.; Lv, Y.J.; Wang, H.X.; Zhang, L.; Wang, K.B.; et al. The dawn of intelligent technologies in tea industry. *Trends Food Sci. Technol.* **2024**, *144*, 104337. [CrossRef]
4. Yang, H.G.; Li, S.W.; Tu, L.J.; Ma, R.R.; Chen, Y. Unsupervised Outlier Detection Mechanism for Tea Traceability Data. *IEEE Access* **2022**, *10*, 94818–94831. [CrossRef]
5. Yang, X.T.; Li, M.Q.; Yu, H.J.; Wang, M.T.; Xu, D.M.; Sun, C.H. A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products. *IEEE Access* **2021**, *9*, 36282–36293. [CrossRef]
6. Xiao, F.; Lai, T.; Guan, Y.T.; Hong, J.M.; Zhang, H.L.; Yang, G.Y.; Wang, Z.F. Application of Blockchain Sharding Technology in Chinese Medicine Traceability System. *CMC-Comput. Mater. Contin.* **2023**, *76*, 35–48. [CrossRef]

7. Varavallo, G.; Caragnano, G.; Bertone, F.; Vernetti-Prot, L.; Terzo, O. Traceability Platform Based on Green Blockchain: An Application Case Study in Dairy Supply Chain. *Sustainability* **2022**, *14*, 3321. [CrossRef]
8. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access* **2019**, *7*, 73295–73305. [CrossRef]
9. López-Pimentel, J.C.; Alcaraz-Rivera, M.; Granillo-Macías, R.; Olivares-Benitez, E. Traceability of Mexican Avocado Supply Chain: A Microservice and Blockchain Technological Solution. *Sustainability* **2022**, *14*, 14633. [CrossRef]
10. Guan, S.P.; Wang, Z.Q.; Cao, Y.L. A Novel Blockchain-Based Model for Agricultural Product Traceability System. *IEEE Commun. Mag.* **2023**, *61*, 124–129. [CrossRef]
11. Xu, X.F.; Bao, X.L.; Yi, H.D.; Wu, J.; Han, J.L. A Novel Resource-Saving and Traceable Tea Production and Supply Chain Based on Blockchain and IoT. *IEEE Access* **2023**, *11*, 71873–71889. [CrossRef]
12. Wu, Y.T.; Jin, X.; Yang, H.G.; Tu, L.J.; Ye, Y.; Li, S.W. Blockchain-Based Internet of Things: Machine Learning Tea Sensing Trusted Traceability System. *J. Sens.* **2022**, *2022*, 8618230. [CrossRef]
13. Paul, T.; Mondal, S.; Islam, N.; Rakshit, S. The impact of blockchain technology on the tea supply chain and its sustainable performance. *Technol. Forecast. Soc. Chang.* **2021**, *173*, 121163. [CrossRef]
14. Paul, T.; Islam, N.; Mondal, S.; Rakshit, S. RFID-integrated blockchain-driven circular supply chain management: A system architecture for B2B tea industry. *Ind. Mark. Manag.* **2022**, *101*, 238–257. [CrossRef]
15. Huang, Y.T.; Liu, H.; Guo, X.X.; Jiao, W.X. The Perception of the National Traceability Platform among Small-Scale Tea Farmers in Typical Agricultural Areas in Central China. *Int. J. Environ. Res. Public Health* **2022**, *19*, 16280. [CrossRef]
16. Chen, C.L.; Zhan, W.B.; Huang, D.C.; Liu, L.C.; Deng, Y.Y.; Kuo, C.G. Hyperledger Fabric-Based Tea Supply Chain Production Data Traceable Scheme. *Sustainability* **2023**, *15*, 13738. [CrossRef]
17. Zou, Y.P.; Peng, T.; Wang, G.J.; Luo, E.T.; Xiong, J.B. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing. *J. Syst. Archit.* **2023**, *144*, 102984. [CrossRef]
18. Xu, G.X.; Dong, J.N.; Ma, C. A certificateless encryption scheme based on blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2952–2960. [CrossRef]
19. Liu, L.; Liu, X.; Wan, J.H. Design of Updating Encryption Algorithm for Privacy Big Data Based on Consortium Blockchain Technology. *J. Math.* **2022**, *2022*, 7138173. [CrossRef]
20. Liang, W.; Zhang, D.F.; Lei, X.; Tang, M.D.; Li, K.C.; Zomaya, A.Y. Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1410–1420. [CrossRef]
21. Feng, T.; Pei, H.M.; Ma, R.; Tian, Y.L.; Feng, X.Q. Blockchain Data Privacy Access Control Based on Searchable Attribute Encryption. *CMC-Comput. Mater. Contin.* **2021**, *66*, 871–884. [CrossRef]
22. Du, R.Z.; Liu, N.; Li, M.Y.; Tian, J.F. Block verifiable dynamic searchable encryption using redactable blockchain. *J. Inf. Secur. Appl.* **2023**, *75*, 103504. [CrossRef]
23. Cheng, J.C.P.; Liu, H.; Gan, V.J.L.; Das, M.; Tao, X.Y.; Zhou, S.J. Construction cost management using blockchain and encryption. *Autom. Constr.* **2023**, *152*, 104841. [CrossRef]
24. Feng, M.Q.; Lin, C.; Wu, W.; He, D.B. SM2-DualRing: Efficient SM2-based ring signature schemes with logarithmic size. *Comput. Stand. Interfaces* **2024**, *87*, 103763. [CrossRef]
25. Fu, J.H.; Zhou, W.H.; Zhang, S.Z. Fabric Blockchain Design Based on Improved SM2 Algorithm. *Int. J. Semant. Web Inf. Syst.* **2023**, *19*, 1–13. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.