Hindawi
Scientific Programming
Volume 2022, Article ID 2604216, 10 pages
https://doi.org/10.1155/2022/2604216

Research Article

Dual-Chain Blockchain in Agricultural E-Commerce Information Traceability Considering the Viniar Algorithm

Zhenjun Xie,[1] **Hua Kong**,[2] **and Bin Wang**[3]

[1]*Chongqing Business Vocational College, School of Electronic Commerce, Chongqing 401331, China*
[2]*Neijiang Normal University, Neijiang 641100, China*
[3]*Shanghai University of Finance and Economics, School of Humanities, Shanghai 200433, China*

Correspondence should be addressed to Zhenjun Xie; share87@163.com and Bin Wang; wangbin@mail.shufe.edu.cn

Received 11 November 2021; Revised 7 December 2021; Accepted 11 December 2021; Published 10 February 2022

Academic Editor: Le Sun

In this paper, we consider the Vennia algorithm to conduct in-depth research and analysis on the traceability of dual-chain blockchain agricultural products' E-commerce information. This paper adds a collaborative verification module to the traceability system and carries out a detailed design of information storage, traceability consensus algorithm, and smart contract for agricultural products according to the characteristics of the agricultural products supply chain, among which the collaborative verification module adopts dynamic data storage technology; the ConsiderVinia consensus algorithm is improved by introducing the way of integral penalty mechanism to ensure the block data validity. After a comparative study of the features and differences of the three major blockchain technology platforms, this paper selects the super ledger to implement the agricultural traceability system based on blockchain technology, introduces the partitioning and credit mechanism into the ConsiderVinia algorithm, and elaborates the improvement process of the algorithm. The improved algorithm reduces the malicious behavior of nodes and maintains the system security through a credit mechanism while maintaining the consistency of blockchain. In the event of a transaction dispute, the third-party platform will determine the party at fault based on the transaction records and other evidence and make corresponding punishments and compensations. The experiment proves that the algorithm proposed in this paper can reduce the amount of network data transmission in the process of node consensus, which is better than the ConsiderVinia algorithm in terms of both throughput and latency, improves the consensus efficiency, and alleviates the communication bottleneck caused by the increase of users in blockchain applications, and the solution of applying the blockchain technology to the agricultural products traceability system is practical and feasible. The blockchain-based agricultural products information traceability system solves the problems of information asymmetry, difficult sharing, easy tampering, and storage centralization in the traditional IoT-based agricultural products traceability system and truly realizes the credible and reliable traceability of the whole chain of agricultural products information. The research content and results of this paper have certain theoretical and practical values.

1. Introduction

E-commerce refers to the business of purchasing goods or services or making digital money transfers over the Internet [1]. The transaction parties jointly trust an authoritative third party to conduct the transaction under the management and supervision of the third party; all user information and transaction information are saved on this third-party server; and in the event of a transaction dispute, the third-party platform will judge the party at fault based on evidence, such as transaction records, and impose appropriate penalties and compensation. The greater convenience, security, liquidity, and cost-effectiveness of E-commerce compared to traditional physical transactions have led to explosive growth in E-commerce transactions each year. The state has provided strong policy support for the development of E-commerce and has specifically enacted an E-commerce law to protect safe transactions. As global food traffic grows, food safety and quality assurance become increasingly important. The modern food supply chain is very complex,

including the cultivation of food, the end retail, and the standardized management of each production process. The food production and processing process contains a large amount of data and involves many participants, each of whom plays a role related to food production. In recent years, there have been outbreaks of foodborne diseases around the world, proliferation of counterfeit and substandard products, and difficulty in pursuing accountability for problems, all of which illustrate the importance of information transparency in food production and distribution process [2]. Through food information traceability, the source of food production and distribution channels can be identified promptly, and the causes of contamination during foodborne disease outbreaks can be understood more quickly. At the same time, highly accurate traceability information can prove whether the requirements are strictly followed during the food distribution process and directly prove the healthiness of the food. In addition, food information can verify the authenticity of food products, and relevant quality parameters can justify the price and reduce the occurrence of food fraud problems. Food information traceability ensures that the food distribution process is under effective monitoring and that problems can be identified promptly for accountability.

With the rapid development of the coordination service industry, the transaction volume is increasing and the transaction data is getting bigger and bigger. However, as each coordination service enterprise has its interests, the transaction data exists in their respective coordination service enterprises and is not disclosed to them. Therefore, the customer cannot easily trace the required data, and the enterprise does not keep the private information of the customer confidential, can also tamper with the internal data privately, and cannot guarantee the security of the data [3]. When customers trade services with coordination service companies, they must enter into relevant agreements with the companies for the required services and the quality of the completed services. If there is a breach of contract by any party in the agreement, the defaulting party is required to compensate the other party. Since the emergence of the coordination service industry, there have been many problems such as loss of goods, noncompletion of goods, and dishonest transactions during coordination transportation. To increase the trust between each other, coordination service enterprises consume more resources when signing relevant agreements or contracts, which further increases the transaction costs and cannot improve the competitiveness of coordination service enterprises [4]. With the rapid development of the coordination service industry, people have put forward higher requirements for coordination service enterprises. If enterprises want to take advantage of the market and improve their competitiveness in the current complex and fiercely competitive environment, further innovation of coordination service transaction systems becomes an inevitable choice.

Among them, the combination of blockchain with various fields has become a hot spot of blockchain research. In this paper, we apply blockchain technology to food information traceability, combine Ethernet blockchain and distributed file storage system IPFS to propose a food information traceability scheme, and design an efficient consensus algorithm for improving the blockchain transaction rate. The growing maturity of blockchain technology can precisely allow the problems in traditional agricultural traceability systems to be solved. The essence of blockchain is a data model, which is characterized using distributed mode. It can also be understood as a ledger, but the recording of this ledger will be shared by all the parties to the transaction. A variety of technologies are encapsulated in the blockchain system, with the support of network communication devices and decentralized servers, and several advanced technologies including timestamps, consensus algorithms, data encryption, and smart contracts are utilized in a convergence of the following: enabling the blockchain to operate securely and smoothly in a centerless network. In terms of functionality and power, any node in the blockchain network is the same without the slightest difference or variation, so all network nodes receive information about the generated blocks at the first time while connecting the latest blocks, which ultimately results in the inconsistency of the entire blockchain network. The existence of the blockchain consensus mechanism makes it possible to keep the data on the chain tamper-evident even when the blockchain network is subject to malicious attacks. This tamper-evident and traceable central less database can solve the problems of product information forgery and information asymmetry during the whole chain flow of agricultural product information collection and transaction. Through blockchain technology, all stakeholders in the flow of agricultural products can be closely involved in the same blockchain network. Such a blockchain model allows every consumer to know the real information about the agricultural products they buy.

2. Related Works

This model uses information collection technologies such as IoT automatic sampling, mobile phone photography, laser scanning, and RFID to achieve full supply chain traceability, but it uses a centralized database for data storage, so the data completely exposed and anyone who has access to the database can make changes to the traceability data, which seriously threatens the credibility of traceability results [5, 6]. However, the system still uses the central database of traceability, which cannot guarantee the authenticity of traceability data and makes the value of the preliminary data collection and data analysis work greatly reduced [7]. High-precision traceability information can prove whether the requirements are strictly followed in the food circulation process, and directly prove the health of the food. In addition, food information can verify the authenticity of the food, and related quality parameters can prove the reasonableness of the price and reduce the occurrence of food fraud. They designed a service-oriented multilayer distributed agricultural traceability model under the guidance of Hazard Analysis and Critical Control Point (HACCP) management system, modularized the system functions, and realized the traceability of quality and safety of agricultural supply chain. In the data layer of the traceability system architecture, the database is divided by function, thereby

reducing the reading burden of a single database, but because it is itself a centralized plaintext database, there is a risk of data tampering, which affects the trustworthiness of traceability results [8].

By using blockchain-powered smart contracts and web service links to reconfigure a user-centric video content delivery system that reduces the cost of video consumption, a blockchain is used to record transaction contracts, a protocol is used to control the completion of the transaction, and the contract is automatically stored in the blockchain for later review and audit [9]. It discusses how blockchain is changing the consumer electronics market, analyzing the winds of change in the now booming multi-billion dollar global consumer electronics industry and potential use cases for electronics. Ultimately, blockchain technology can make the consumer electronics industry more transparent, secure, and honest. Account information in the account blockchain and transaction activity in the transaction blockchain are stored separately and distributed. The virtual account of the account is used for transactions to protect account information from being leaked [10]. Although there has been a lot of research on various directions of blockchain, there is little literature so far on blockchain transactions and regulation and verification of smart contracts; therefore, this paper proposes a regulatory verification model for smart contracts using an improved Virginia encryption algorithm combined with the use of asymmetric algorithms to store smart contracts cryptographically for sale on the chain of custody market, forming a profit model that incentivizes users to improve smart contract diversity, and providing an economic basis for regulatory verification of smart contracts and a mass basis for further development of blockchain [11].

In the Internet era, online transactions are prevalent; however, the current centralized transaction model brings many problems, such as leakage of users' private information, excessive third-party rights, proliferation of fake goods and fake networks that are not easy to distinguish, high pressure on central server storage, and exposure to various hacker attacks. In this paper, we summarize the root causes of these problems in traditional E-commerce and compare the differences between blockchain transactions and traditional E-commerce transactions. Through comparison and analysis, we determine that blockchain, which uses a distributed system that can ensure data is not tampered with, transaction information is open and transparent, and personal information is encrypted and saved and can realize anonymous transactions, can solve some shortcomings of the traditional E-commerce transaction model.

3. Improved Two-Chain Blockchain E-Commerce Information Analysis for Agricultural Products considering the Vennia Algorithm

3.1. Improved Algorithm to Consider the Vennia Algorithm. Asymmetric encryption algorithms usually have a complex computation process, and the security is highly dependent on the length of the key, so the key is usually long and consumes more arithmetic power, and the encryption and decryption speed are relatively slow, but it is also more secure [12]. If the security of the private key can be guaranteed, the security of the data can be guaranteed, so it is suitable for encrypting a small amount of content, and the key does not need to be changed frequently. Symmetric encryption algorithms, on the other hand, are relatively simple and have shorter key lengths, so the keys are cheaper to transmit and compute, and the algorithms run quickly and efficiently. Because the encryption and decryption keys of symmetric encryption algorithms are the same or can be easily derived from each other, the keys need to be changed frequently. The encryption process of stream cipher is as follows: first, a keystream is generated from the original key K and a random number using a certain algorithm; then, the plaintext stream and the keystream are used to generate the ciphertext using an encryption algorithm. The longer the period of the keystream and the more even the frequency distribution, the higher the resistance to frequency analysis attacks and the more secure it is; even its ideal degree of primary cipher algorithm can achieve unbreakable security, but this is only theoretically feasible; all we can do is to try to get closer to the primary cipher to enhance security. In addition, internal data can be tampered with privately, and data security cannot be guaranteed. When a customer conducts a service transaction with a coordination service company, he/she must sign an agreement with the company on the required service and the quality of the service.

$$c = Ek_1\left(m_1^2\right)Ek_2\left(m_2^2\right)\cdots Ek_i\left(m_1^2\right), \tag{1}$$

$$C_i = \left(P_i^2 - K_i^2\right) \bmod \{26\}. \tag{2}$$

The cipher was considered secure for quite some time, but its myth was eventually shattered. It was discovered that if the plaintext was much longer than the length of the cipher key, analyzing the frequency of the cipher letters could help find out the length of the key, and the cipher could then be easily decrypted.

$$EK\left(P_1, P_2, \ldots, P_m\right) = \left(P_i^2 - K_i^2 + P_i - K_i\right) \bmod \{92\}. \tag{3}$$

However, this approach increases the size of the ciphertext so that it takes up too much space when many messages need to be transmitted securely [13]. Therefore, we propose a new encryption method combining Vigenère cipher, LFSR, and OTP that enables the letters in the ciphertext to be evenly distributed and does not change the size of the ciphertext, as shown in Figure 1.

The length of the new key period must exceed the length of the plaintext to ensure that the key is not repeated and to prevent frequent attacks. Experimentally, the formula proposed in this paper proves to be achievable because our new key has a fixed period, but the period is long enough. For example, it is calculated that if the length of the original password is 3, the period length will be 168. There are problems such as lost goods, uncompleted goods, and dishonest transactions. In this regard, problems such as the lack of trust between the participants in the coordination service transaction contract have appeared in the coordination

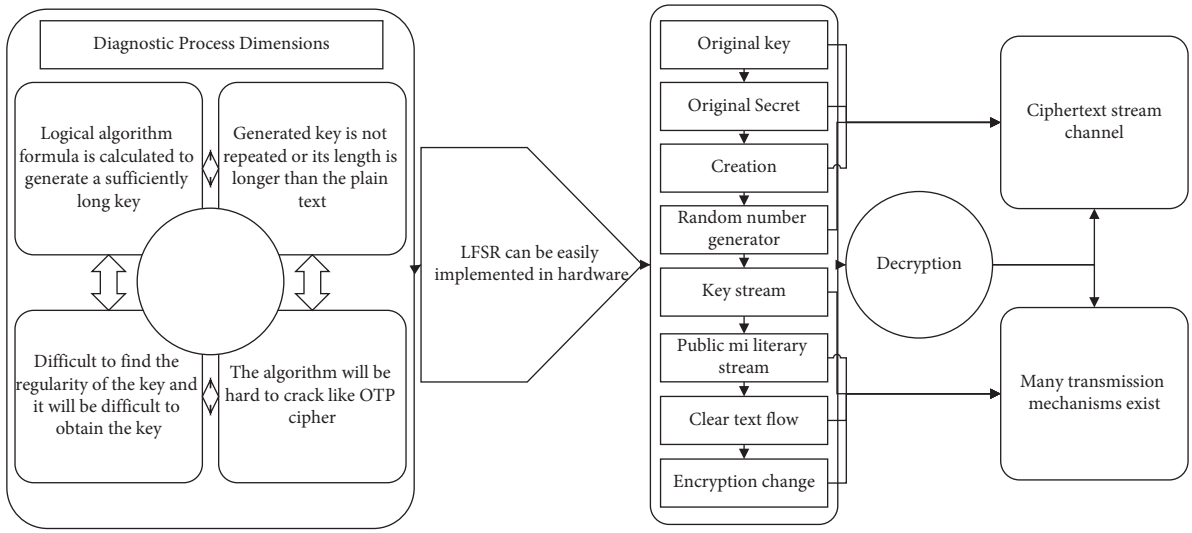

Figure 1: Improved framework for considering the Vennia algorithm.

service transaction. The period will grow nonlinearly with the length of the original password. The second advantage of the new algorithm is that it can completely hide the frequency characteristics of the letters in the ciphertext, achieving a near-average distribution of ciphertext letters [14]. Although both the time complexity and space complexity of the improved algorithm have been improved, the improvement is within an acceptable range and its security has been significantly improved.

$$IC = \frac{\sum_{i=a}^{i=z} f_i\left(f_i + 1\right)}{N\left(N + 1\right)}. \tag{4}$$

Very short keys produce very long cycles, and if the cycle length of the new key generated is greater than the plaintext length, the length of the original key has little effect on the frequency distribution of the final ciphertext. Therefore, the original key with a short length can be chosen within the cycle range to save resource consumption during transmission. We further analyze the data to compare the two encryption algorithms, and compare them to the traditional Vigenère cipher; we can see that the new algorithm has a smaller alphabetic overlap index based on the experimental results. The chi-square test is the degree of statistical sample deviation between the actual observed values of the data and the theoretical values inferred through computation.

$$x^2 = \sum_{\mathrm{i}=1}^{k} \frac{\left(A_i + E_i\right)^2}{E_i^2}, \tag{5}$$

$$D\left(X\right) = \sum_{\mathrm{i}=1}^{n} p_i\left(x_i^2 + \mu\right)^2. \tag{6}$$

In addition, there is a small improvement in the values when the length of the cipher is increased from 4 to 5.

In supply chain management, blockchain technology-based supply chain management can ensure the openness and transparency of each transaction data, and the main information flow of the whole complete supply chain is kept on the blockchain, which provides a guarantee for timely detection of problems and targeted problem-solving in each link and thus improves the efficiency of supply chain management. Secondly, the timestamp of blockchain can provide evidence and proof of existence for the dispute resolution of each participant [15]. Finally, the combination of data tampering ability and transaction traceability can ensure the authenticity and reliability of the data on the chain, which can effectively reduce the phenomenon of product counterfeiting, as shown in Figure 2. We combine the Ethereum blockchain and the distributed file storage system IPFS to propose a food information traceability plan, and design an efficient consensus algorithm to increase the transaction rate of the blockchain.

The cultural entertainment field based on blockchain technology proves the authenticity of the existence of a work, an article, etc. through hash algorithm and timestamp, and when the work is uploaded to the blockchain and has been verified, the subsequent transactions of the work will be recorded in real time, which provides strong technical support for the proof. Secondly, the cultural entertainment based on blockchain technology can organically integrate the various parts related to it Finally, blockchain-based technology in the field of culture and entertainment can increase the protection and supervision; realize the consensus between individuals and individuals, individuals and industries, and industries and industries; etc., which will continuously enhance the standardization, self-awareness, and reliability of the industry and at the same time strongly reduce the occurrence of infringement and piracy.

OTP is secure and, although impossible to implement, can provide ideas for our new algorithm. The experimental analysis shows that the new algorithm is secure in frequency analysis attacks because the key period is larger than the plaintext length [16].

3.2. Dual-Chain Blockchain E-Commerce Information Traceability Design for Agricultural Products. In the food information traceability scheme, the supplier grows raw

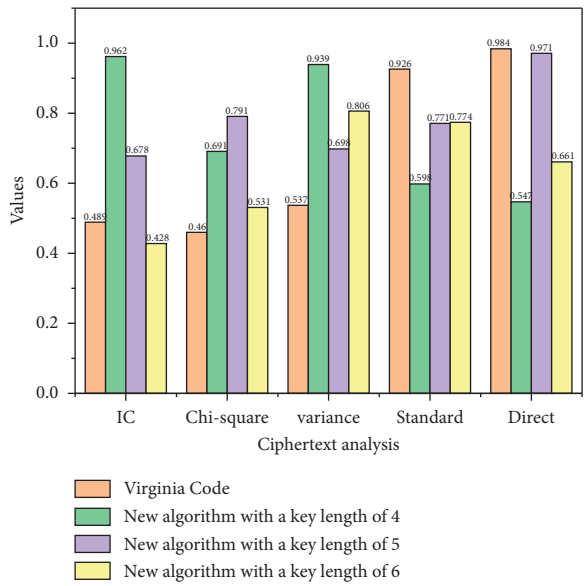

Figure 2: Ciphertext analysis.

materials and provides them to the producer, who needs to complete the registration of raw materials in the system, use a unique identification code to identify the raw materials, and provide detailed information during their growth and storage, such as temperature, humidity, and geographical location, so that consumers can easily trace the source of food materials. The producer buys the raw materials from the supplier, processes the raw materials to obtain the food, and provides it to the distributor, who then sells it worldwide. In the process of food production, producers need to record the production environment, source of materials, production process, quarantine information and other production process information; use the international coding standard EAN/UCC-13 to code the food; package the food by batch; and register the food information;, the same batch of products corresponds to a production batch number [17]. As an intermediary to transfer food from producers to consumers, distributors record the flow of food in the process of food transfer to ensure the continuity of food information in the process of information traceability; retailers buy products in bulk from distributors, then sell them to consumers in retail mode, and have a direct transaction relationship with consumers. Therefore, all network nodes will receive the generated block information in the first time, at the same time connect to the latest block, and finally form the uniformity of the entire blockchain network.

The process of food information traceability needs to achieve end-to-end traceability, and nodes need to update food transfer information promptly to prevent information breakage, ensure the relevance of traceability information, and cover the whole process of food circulation. As a design to support the traceability of food information, after the food information involved in the supply chain and the process information of food circulation are put into the blockchain, the data is open to the whole network, the two parties involved in the transaction can obtain relevant data by querying the transaction information, and the regulator is also able to quickly investigate and locate the responsible person through the obtained information when problems arise. To achieve traceability of food information, data and transaction information of food products at all stages of circulation from raw materials to production to distribution and retail need to be written into the blockchain to provide proof of information origin [18] (Figure 3).

Raw material suppliers and producers enter new data collection in the process of raw material cultivation and food production, using sensors, radio frequency identification (RFID), electronic cameras, and other technologies to collect crop growth and food production process information in a noncontact way. Since only single text information can be stored in blockchain, IPFS distributed storage system is introduced to store data such as pictures and files in the IPFS database and upload the returned file hash to blockchain storage. In this paper, Ethernet is used as the underlying blockchain platform, which has a turing-complete instruction set, supports multiple languages, and provides a good environment for smart contract development. To facilitate data writing and information query in the blockchain, this paper designs multiple smart contracts to implement these functions. In the design of this paper, raw material suppliers and manufacturers use data storage contracts to add product information and maintain a mapping relationship between product information and transaction update contract addresses. The supplier adds raw material information to the data storage contract, and the producer writes information about each batch of food produced in the contract so that it can be queried by other nodes [19].

Every transaction after the food leaves the producer must be written into the blockchain through a smart contract, and when users perform transaction information update, in addition to judging the user's authority through the authorization list, they need to judge the validity of the transaction hash when entering the previous transaction hash to prevent users from falsifying transaction information. The final consumer can obtain all the transaction records of food circulation through the transaction hash and precisely query the transit node of each batch of food circulation. The coordination service provider completes the service to the coordination service user according to the smart contract conditions [20]. After the service is completed, the smart contract automatically sends the service fee to the account of the coordination service provider.

All closely focus on the same blockchain network to perform related operations. Such a blockchain model allows every consumer to know the real and relevant information about the agricultural products they buy. In this agricultural product traceability system model, the production data of agricultural products are collected by video monitoring, temperature and humidity sensors, concentration sensors, and other equipment in the production and planting process; the information of agricultural product processing is collected and recorded by sensing chips and product identification in the harvesting and processing process; the transportation process is collected and recorded by positioning devices and environmental monitoring equipment

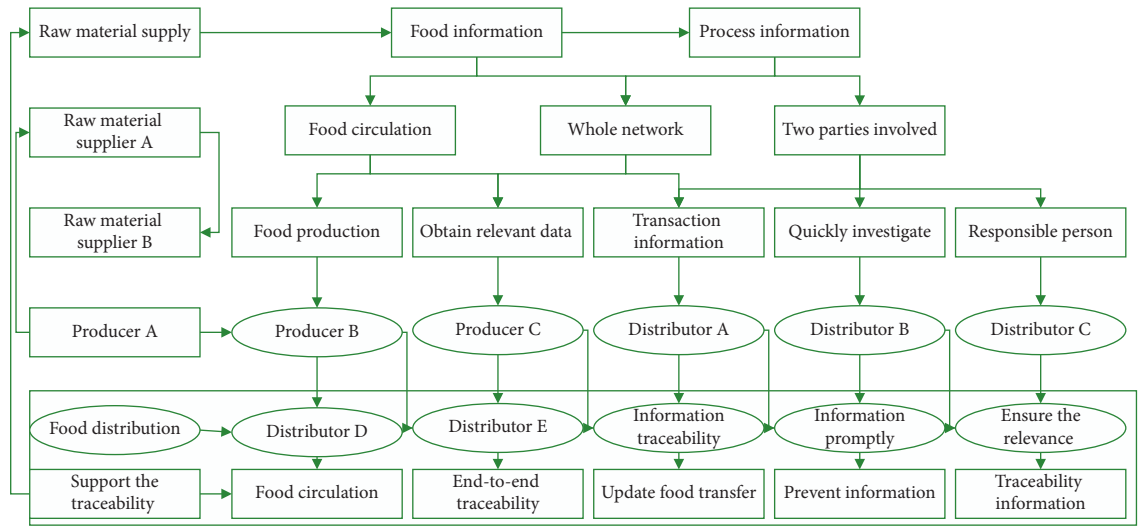

Figure 3: Supply chain and traceability queries.

in the transportation process; and the environmental data of agricultural products in the transportation process is collected and recorded by environmental monitoring equipment in the logistics and transportation process. The sales link uses barcodes and QR codes to record the sales data of agricultural products. The data of each link is verified and stored on the blockchain network. After the traceability information of agricultural products is stored on the chain, the cryptographic encryption technology is used to encrypt the uploaded data to prevent the producer of agricultural products or the coordination turnover from tampering with the information of agricultural products, and the timestamp in the blockchain technology is relied on to realize the traceability of information related to agricultural products. Relying on the timestamp technology in the blockchain system to generate a blockchain for traceability inquiry and supervision, the chain runs through the agricultural products from planting to selling, and the status of the products can be inquired through the chain at any time, as shown in Figure 4.

The decentralized model of coordination service transaction proposed in this paper intelligently matches coordination service users with coordination service providers according to the services they need and provide, reduces the tedious manual transaction matching operation in the process of coordination service transaction, and realizes intelligent transaction matching [21]. In the case of information asymmetry among information service providers, the initial stage of blockchain establishment depends on the effort of the transporters. An incentive mechanism contract model based on the constraints of information service providers is established.

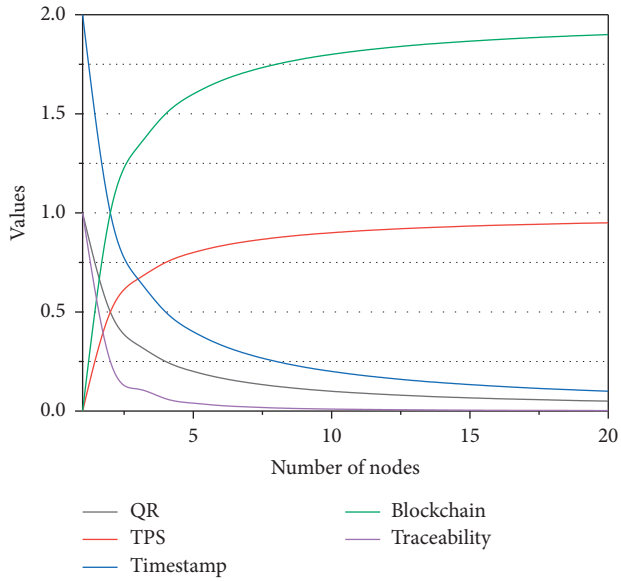

Figure 4: TPS mean curve.

4. Analysis of Results

4.1. Considering the Performance of the Vennia Algorithm. Intermediary attacks emerged early but have never been completely solved, mainly because they are very stealthy and difficult to prevent. When the man-in-the-middle attack is sent, the network runs normally without interruption, no Trojan horse or malware is detected on the computer, and the attacked persons think they are communicating normally with safe objects, so they will be undefended and leak a lot of information, making it easy for the attacker to steal or even tamper with important information, causing significant losses. In traditional E-commerce, users rely on CA certificates issued by third parties to confirm the identity of transaction objects and use SSL protocols to ensure data security; however, these measures cannot completely defend against man-in-the-middle attacks, especially for some ordinary users who do not understand the relevant expertise and for whom it is difficult to distinguish attackers from real traders. The symmetric encryption algorithm is relatively simple, and the key length is shorter, so the transmission and calculation cost of the key is lower, and the algorithm runs fast and efficient. A dual-chain blockchain can achieve the

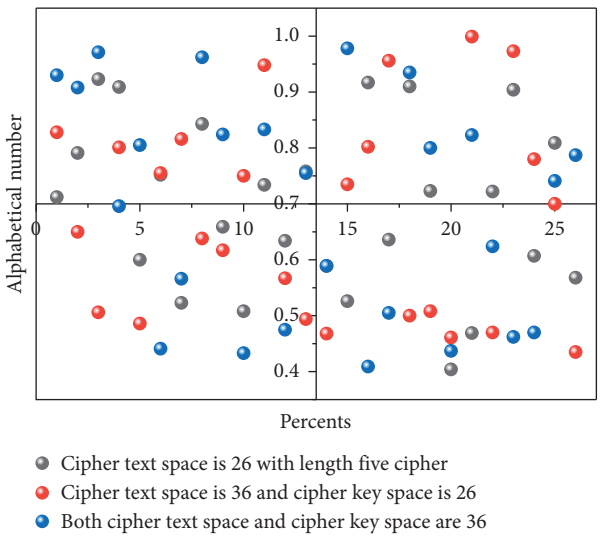

Figure 5: Frequency comparison of different encryption spaces.

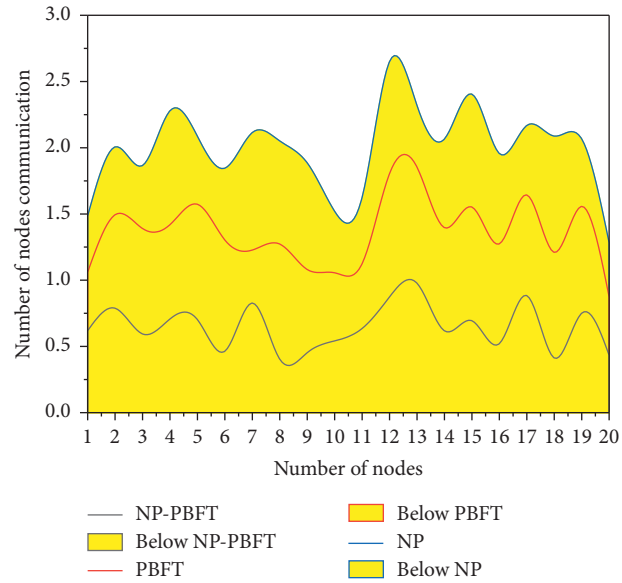

Figure 6: Single transaction traffic.

effect of preventing the man-in-the-middle attack. The user's identity is determined in blockchain by digital signature or zero-knowledge verification, and the digital signature is unforgeable according to its hash characteristics. The zero-knowledge proof is what allows users to achieve the effect of anonymous transactions, and it is robust, unforgeable, and unstealable. As a result, MITM, which attacks by impersonating identities between two parties to a transaction, will no longer be effective, as shown in Figure 5.

All data in the blockchain is commonly recognized and preserved through nodes across the network, making it impossible for identity information to be tampered with and stolen unless it is subjected to a 51% attack, which is also known as Byzantine fault tolerance. In a dual-chain blockchain, the chain of custody also backs up the data saved in the transaction chain, scaling the ledger further and increasing security. Secondly, there are timestamps in each block that records when transactions occur in real time, and it is also not feasible to try to obscure ownership by obfuscating the concept of time. What is more, the distributed architecture of blockchain determines that it is pooling the arithmetic resources of all nodes to work together, so DDoS attacks against servers can also be defended by connecting users to a nearby pool of protection resources.

It includes the encryption process of the sender, the decryption process of the receiver, and the transmission process of the ciphertext key. There are many transmission mechanisms used to ensure transmission security in the network. The entropy value of the ciphertext shows that the expansion of the ciphertext space greatly increases the uncertainty of the ciphertext characters. If the ciphertext space contains only 26 symbols and is encrypted with a key length of 5 characters, the entropy of the ciphertext is 4.6734. When the ciphertext space is expanded to 36 symbols, the entropy of the ciphertext is 5.0824. When the key space is also expanded to 36 symbols, the entropy of the ciphertext is 5.1289, which is greater than the other two values. This indicates that the ciphertext becomes more secure. The distribution of symbols in the ciphertext will be more uniform as shown in Figure 6.

It is possible to select an existing suitable smart contract from the chain of custody for use at a very low price, or you can draw up your personalized smart contract and submit it to the chain of custody for legitimacy verification. After the personalized smart contract provided by the user is verified, both the contract provider and the contract verifier are paid a percentage if it is used by subsequent traders. This provides an incentive for individual users to actively provide personalized smart contracts, as well as to make further improvements in the multiple uses of the smart contract, which can be profitable. C2C transactions can be carried out on the public chain because it uses a fully distributed system with many nodes and a neutral and open internode system that enjoys the same level of privacy. B2C and B2B E-commerce transactions can be implemented on a federated chain or a private chain, because both transaction models are generally designed for larger amounts and more frequent transactions. Combined with smart contracts, it can ensure that the transaction participants conduct transactions according to the predetermined rules, and the chain of custody supervises and maintains the rights of the transactions, thus ensuring that the transactions are legal and effective.

4.2. Dual-Chain Blockchain Agricultural E-Commerce Information Traceability Results. To test the transaction latency of the algorithm, an experiment is conducted by the client continuously initiating a transaction request and recording the time taken for each consensus to complete. For the accuracy of the experiment, the average value of 100 transaction latencies is taken as the transaction latency of the algorithm and tested with a different number of nodes to get the result. In addition, selection-based practical Byzantine fault tolerance (SPBFT) algorithm is used as an experimental comparison. SPBFT algorithm divides the nodes into

Table 1: Matching results and overall utility values.

Matching result	Overall utility value	Matching result	Overall utility value
Y1-X1	0.986	Y6-X6	0.758
Y2-X2	0.471	Y7-X7	0.906
Y3-X3	0.698	Y8-X8	0.719
Y4-X4	0.955	Y9-X9	0.627
Y5-X5	0.475	Y10-X10	0.864

consensus nodes and candidate nodes, and only a few consensus nodes are selected to execute simplified consistency protocol when there are no faulty nodes; otherwise, all the nodes are judged by simplified consistency protocol after nodes execute PBFT consistency protocol to complete consensus. In Table 1, for users to perform multiobjective matching of coordination service transactions, the transaction matching result pairing and the overall utility value of matching are shown. The data in the table indicates that both matching parties are more satisfied with the matching results, and then smart contracts are generated based on the matching results.

The coordination service user and the coordination service provider obtain the total matching result through the algorithm-matched transactions. The experiment takes a week as an example, during which the system matches a coordination service user with a coordination service provider a total of 4432 times, with 3961 successful matches, 471 failed matches, and a success rate of approximately 89.37%. Table 1 shows smart contracts in a multinode blockchain network. The experiment time is also taken as one week, during which the system signed a total of 3131 smart contracts for successfully matched counterparties, with 75 failed contracts and approximately 97.60% valid smart contracts. Furthermore, the average confirmation time for each transaction payment at the end of the service when the contract is executed is about 30 s. From the above experimental results, it is concluded that the proposed smart contract algorithm and transaction mechanism for coordination service transaction ant colony are feasible and effective in solving the problems of intelligent coordination service transactions, data centering of transactions, and lack of smart contracts for multiple transactions. The global optimal mean change curve of the overall satisfaction function and the matching evaluation function is obtained. The above results show that the improved ant colony algorithm proposed in this paper is feasible and effective and can better solve the multiobjective transaction matching problem, as shown in Figure 7.

We save the resource consumption during transmission and further compare the two encryption algorithms through data analysis. Compared with the traditional Vigenère password, according to the experimental results, the letter overlap index of the new algorithm is smaller. Chi-square test is the degree of deviation of the statistical sample between the actual observation value of the data and the theoretical value through calculation. The expected earnings of transporters all increase as their transport capacity increases; i.e., they can ensure that transport enterprises with greater transport capacity have greater earnings than those

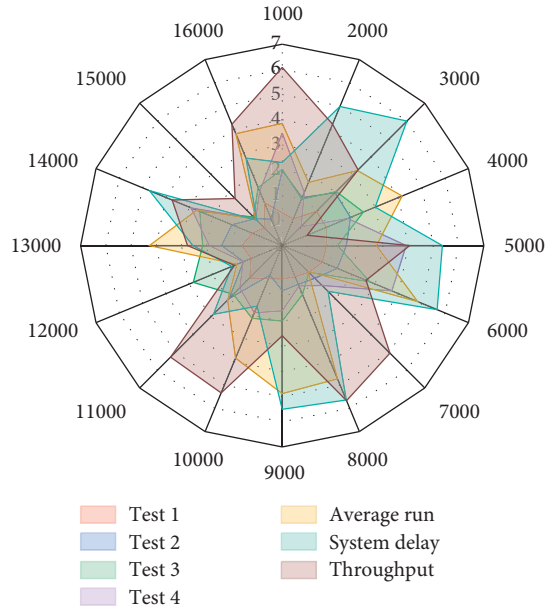

Figure 7: System performance under query requests.

with relatively weak transport capacity. Enterprises always aim at profitability, so whether the mixed contract or separate contract incentive mechanism is signed between information service providers and transporters, it will motivate transporters to make efforts to improve their transport capacity, for example, by increasing the expenditure on information technology equipment, developing information technology enterprise support system, improving the quality of logistics services from the customer's perspective, and establishing a logistics service quality satisfaction evaluation system. Thereby, the information service providers use incentive contracts to achieve efficient incentives for transport enterprises on the blockchain and increase transporters' motivation.

Figure 7 shows the system throughput under query requests, and the system throughput stabilizes at about 350 when the query requests increase from 1000 to 10000.

5. Conclusion

In this paper, the Virginia cipher is improved, and it is demonstrated using data analysis that this algorithm can secure plaintexts at a lower cost and with higher security. The drawback of this algorithm is that it requires the key to be sent to the transacting party securely, and hence it can be applied in combination with asymmetric encryption. The plaintext is encrypted with this algorithm; the asymmetric

encryption algorithm is used to encrypt the short key, thus reducing the cost of encryption and decryption and reducing the waste of arithmetic and storage resources; and the key can be easily replaced, which is suitable for the sale of electronic goods in the network. The cultural and entertainment field based on blockchain technology can increase protection and supervision; realize multidimensional consensus issues between individuals and individuals, individuals and industries, and industries and industries; and will continue to improve the standardization, consciousness, and reliability of industries. At the same time, it effectively reduces the occurrence of infringement and piracy. In this paper, the centralized traceability model of agricultural products is decoupled into a distributed blockchain model composed of supporting functional modules; the flexible traceability model of agricultural products based on blockchain is obtained; and the operational mechanisms of edge users, dynamic tracking, fast traceability and the release and accountability scheme of traceability data are designed according to the characteristics of this model to further improve the flexibility of traceability process and the credibility of traceability results. Finally, this paper designs the architecture of the traceability system based on this model and realizes a blockchain-based flexible traceability system for agricultural products. On the one hand, the blockchain technology is combined with the traceability system of agricultural products, and the corresponding system design is proposed, and on the other hand, a scheme for the implementation of the blockchain-based traceability system of agricultural products is proposed.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

The research was supported by "Application Research of Block Chain Technology in Agricultural E-Commerce Traceability System under Digital Rural Construction," project of 2021 Science and Technology Research Program of Chongqing Education Commission of China (No. KJQN202104401).

References

[1] Z. Zhang, S. Geiger, M. Rood et al., "A tracing algorithm for flow diagnostics on fully unstructured grids with multipoint flux approximation," *SPE Journal*, vol. 22, no. 6, pp. 1946–1962, 2017.

[2] R. Sun, G. Wang, Z. Fan, T. Xu, and W. Y. Ochieng, "An integrated urban positioning algorithm using matching, particle swam optimized adaptive neuro fuzzy inference system and a spatial city model," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4842–4854, 2020.

[3] N. Hirnschall, T. Buehren, M. Trost, and O. Findl, "Pilot evaluation of refractive prediction errors associated with a new method for ray-tracing–based intraocular lens power calculation," *Journal of Cataract & Refractive Surgery*, vol. 45, no. 6, pp. 738–744, 2019.

[4] V. V. Sanzharov and V. A. Frolov, "Level of detail for precomputed procedural textures," *Programming and Computer Software*, vol. 45, no. 4, pp. 187–195, 2019.

[5] M. Schneider, P. Bartko, W. Geller et al., "A machine learning algorithm supports ultrasound-naïve novices in the acquisition of diagnostic echocardiography loops and provides accurate estimation of LVEF," *The International Journal of Cardiovascular Imaging*, vol. 37, no. 2, pp. 577–586, 2021.

[6] I. Caetano, L. Santos, and A. Leitão, "Computational design in architecture: Defining parametric, generative, and algorithmic design," *Frontiers of Architectural Research*, vol. 9, no. 2, pp. 287–300, 2020.

[7] A. K. Sales, E. Gul, M. J. S. Safari, H. G. Gharehbagh, and B. Vaheddoost, "Urmia lake water depth modeling using extreme learning machine-improved grey wolf optimizer hybrid algorithm," *Theoretical and Applied Climatology*, vol. 146, no. 1, pp. 833–849, 2021.

[8] R. He, B. Ai, A. F. Molisch et al., "Clustering enabled wireless channel modeling using big data algorithms," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 177–183, 2018.

[9] T. Ali, S. Yasin, U. Draz, and M. Ayaz, "Towards formal modeling of subnet based hotspot algorithm in wireless sensor networks," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1573–1606, 2019.

[10] W. Xue, K. Yu, X. Hua, Q. Li, W. Qiu, and B. Zhou, "APs' virtual positions-based reference point clustering and physical distance-based weighting for indoor Wi-Fi positioning," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3031–3042, 2018.

[11] F. Leal, B. Malheiro, B. Veloso, and J. C. Burguillo, "Responsible processing of crowdsourced tourism data," *Journal of Sustainable Tourism*, vol. 29, no. 5, pp. 774–794, 2020.

[12] M. Lindner, J. Rosenow, and H. Fricke, "Aircraft trajectory optimization with dynamic input variables," *CEAS Aeronautical Journal*, vol. 11, no. 2, pp. 321–331, 2020.

[13] Z. Wang, X. Li, and X. Shang, "Distribution characteristics of mining-induced seismicity revealed by 3-D ray-tracing relocation and the FCM clustering method," *Rock Mechanics and Rock Engineering*, vol. 52, no. 1, pp. 183–197, 2019.

[14] J. S. Li, I. H. Liu, C. Y. Lee, C. F. Li, and C. G. Liu, "A novel data deduplication scheme for encrypted cloud databases," *Journal of Internet Technology*, vol. 21, no. 4, pp. 1115–1125, 2020.

[15] J. Teng and H. Ma, "Dynamic asymmetric group key agreement protocol with traitor traceability," *IET Information Security*, vol. 13, no. 6, pp. 703–710, 2019.

[16] F. Belkadi, J. Le Duigou, L. Dall'Olio, G. Besombes, and A. Bernard, "Knowledge-based platform for traceability and simulation monitoring applied to design of experiments process: an open source architecture," *Journal of Engineering Design*, vol. 30, no. 8-9, pp. 311–335, 2019.

[17] F. Li, H. Li, B. Niu, and J. Chen, "Privacy computing: concept, computing framework, and future development trends," *Engineering*, vol. 5, no. 6, pp. 1179–1192, 2019.

[18] T. Sato, Y. Iwamoto, S. Hashimoto et al., "Features of particle and heavy ion transport code system (PHITS) version 3.02," *Journal of Nuclear Science and Technology*, vol. 55, no. 6, pp. 684–690, 2018.

[19] G. Wu, K. Wang, J. Zhang, and J. He, "A lightweight and efficient encryption scheme based on LFSR," *International Journal of Embedded Systems*, vol. 10, no. 3, pp. 225–232, 2018.

[20] S. Dong, "Improved label propagation algorithm for overlapping community detection," *Computing*, vol. 102, no. 10, pp. 2185–2198, 2020.

[21] R. He, Q. Li, B. Ai et al., "A kernel-power-density-based algorithm for channel multipath components clustering," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7138–7151, 2017.