Hindawi
Security and Communication Networks
Volume 2022, Article ID 2958963, 11 pages
https://doi.org/10.1155/2022/2958963

Research Article

BCST-APTS: Blockchain and CP-ABE Empowered Data Supervision, Sharing, and Privacy Protection Scheme for Secure and Trusted Agricultural Product Traceability System

Guofeng Zhang,[1] **Xiao Chen**,[2] **Bin Feng**,[1] **Xuchao Guo**,[3] **Xia Hao**,[4] **Henggang Ren**,[1] **Chunyan Dong**,[1] **and Yanan Zhang**[5]

[1]*School of Information Science and Technology, Taishan University, Taian, Shandong 271000, China*
[2]*School of Economics and Management, Taishan University, Taian, Shandong 271000, China*
[3]*College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China*
[4]*College of Information Science and Engineering, Shandong Agricultural University, Taian, Shandong 271000, China*
[5]*School of Information Science and Engineering, University of Jinan, Jinan, Shandong 250022, China*

Correspondence should be addressed to Guofeng Zhang; zhangguofeng@tsu.edu.cn and Bin Feng; binfeng@tsu.edu.cn

Received 23 October 2021; Revised 1 December 2021; Accepted 24 December 2021; Published 15 January 2022

Academic Editor: Yuling Chen

Blockchain provides new technologies and ideas for the construction of agricultural product traceability system (APTS). However, if data is stored, supervised, and distributed on a multiparty equal blockchain, it will face major security risks, such as data privacy leakage, unauthorized access, and trust issues. How to protect the privacy of shared data has become a key factor restricting the implementation of this technology. We propose a secure and trusted agricultural product traceability system (BCST-APTS), which is supported by blockchain and CP-ABE encryption technology. It can set access control policies through data attributes and encrypt data on the blockchain. This can not only ensure the confidentiality of the data stored in the blockchain, but also set flexible access control policies for the data. In addition, a whole-chain attribute management infrastructure has been constructed, which can provide personalized attribute encryption services. Furthermore, a reencryption scheme based on ciphertext-policy attribute encryption (RE-CP-ABE) is proposed, which can meet the needs of efficient supervision and sharing of ciphertext data. Finally, the system architecture of the BCST-APTS is designed to successfully solve the problems of mutual trust, privacy protection, fine-grained, and personalized access control between all parties.

1. Introduction

Food for the people: food safety is the first and most important. From a global perspective, food safety incidents are typical public health emergencies. In order to solve those, countries around the world have successively studied and established a variety of APTSs relying on the agricultural product supply chain, mainly using the centralized technical architecture to realize the shared storage of traceability data. However, frequent privacy leaks in the data center and frequent food safety incidents have led consumers to lose trust in the traceability system. At the same time, considering many factors such as data ownership, data leakage, and their own commercial interests, agricultural production enterprises or organizations with a large amount of data are extremely cautious about opening their own internal data, especially core data. When food safety incidents break out, data are not available, tampered, or maliciously forged from time to time, resulting in the problems of less data and low reliability of agricultural product traceability system (APTS).

The main reasons for the above problems are as follows. Firstly, the data privacy of the participants in the supply chain is not effectively protected, resulting in the difficulty of

establishing a trust relationship between the participants. Secondly, regulators lack safe and effective regulatory technical means to effectively supervise the complete supply chain data. Finally, consumers no longer trust existing traceability systems and technologies. It can be seen that the contradiction between data privacy protection and efficient sharing of APTS is becoming increasingly prominent, and the problem of data security is still the difficulty and pain point restricting the safe sharing and supervision of agricultural products traceability data. The reason lies in the imperfect data privacy protection and access control technology of the traceability system.

The decentralization, nontampering, and traceability of blockchain technology provide new technologies and ideas for the construction of APTS. Based on blockchain and CP-ABE encryption technology, this paper constructs a secure and trusted agricultural product traceability system (BCST-APTS), which can meet the whole supply chain data supervision, fine-grained authorized access control, and secure and trusted data sharing.

The main contributions of this paper are as follows:

(1) With the help of cryptographic algorithms, the data stored on the blockchain can be encrypted to ensure data privacy and completely solve the trust problem between consumers and system participants.

(2) Based on CP-ABE encryption technology, it provides new technical means to solve the problems of privacy protection, fine-grained access control, and data supervision of agricultural product supply chain data.

(3) The proposed attribute management infrastructure scheme can more efficiently and flexibly meet the personalized privacy protection needs of supply chain participants.

(4) A RE-CP-ABE scheme is proposed and elaborated in detail, which can quickly and accurately determine data access rights. More importantly, it can meet the data supervision requirements of the supervisory organization for the entire supply chain.

2. Related Works

2.1. Agricultural Product Traceability System Based on Blockchain. Graves et al. [1] believe that the three processes of production, transportation, and sales are the core, and integrated production, information sharing, and production operations are an important research direction of the supply chain. Cachon and Fisher [2] believe that information sharing can effectively improve the operational efficiency of the supply chain. Boehlje et al. [3] believe that building a traceability system for agricultural products can effectively reduce the cost of food supervision and improve the quality of products. Gao et al. [4] believe that the establishment of trust mechanisms and information sharing mechanisms should be accelerated between all entities in the supply chain, and an information service platform should be built to realize corporate information sharing, so as to reduce the overall operating costs of the supply chain and improve the operating efficiency and economic benefits of the supply chain. However, the existing data sharing and traceability system, which mainly adopts centralized technology architecture construction, can no longer be accepted by consumers. More precisely, the actual value of the traceability system is gradually being weakened.

The system architecture based on blockchain technology has the characteristics of decentralization, nontampering, traceability, etc., which can not only meet the traceability requirements of the entire process of the agricultural product supply chain, but also realize the distributed shared storage of agricultural product entire process data. Agricultural blockchain technology can make traceable information fairer, just, transparent, lightweight, and efficient to reach consensus [5]. However, the consensus mechanism is a key technology to achieve consensus between organizations and nodes on the chain, and its vulnerability may damage the entire blockchain system [6, 7]. Liu et al. [8] designed an anticounterfeiting traceability system based on blockchain technology that combines public and private chains to ensure the authenticity and reliability of the traceability information obtained and solve the problem of difficult supervision of traditional traceability systems. Feng [9] established an agricultural food supply chain traceability system based on RFID and blockchain technology. The system covers all links of the agricultural product supply chain, including the whole process of data acquisition and information management, and realizes the quality and safety monitoring, tracking, and traceability management of agricultural products "from farm to table." Yang et al. [10] designed a "database + blockchain" agricultural product traceability information storage model and query method based on hyperledger fabric, and the encrypted hash value of traceability data is stored on the blockchain.

The above research successfully focused on the system architecture design and function realization, realized the distributed storage of agricultural product data, and ensured the data integrity. However, the existing research lacks in-depth research on data confidentiality, secure storage, access control, etc., cannot protect the data and privacy of entities in the traceability system, and is difficult to apply in practice.

2.2. Privacy Protection and Access Control of Blockchain. According to the degree of openness of the blockchain system, it can be divided into Public Blockchain, Private Blockchain, and Consortium Blockchain. According to whether the access of the organization node needs to be licensed, it can be divided into Public Blockchain and Permissioned Blockchain. Obviously, nonpublic Blockchains such as Consortium Blockchain and Private Blockchain are called Permissioned Blockchain [11]. Since the Permissioned Blockchain is a type of blockchain that each node needs to be licensed by the regulatory agency or authoritative organization, after verifying the identity, it is assigned specific system permissions to carry out specific businesses. Compared with the Public Blockchain, the Permissioned Blockchain is more suitable for application

scenarios that require supervision, cross-organization sharing, and multiparty business collaboration.

For any industry, users are unwilling to share their personal information and confidential data with competitors [12], such as source location privacy [13]. The design of the agricultural product supply chain scheme based on the blockchain should ensure the security and credibility of data encryption storage, transaction records can be traced, inquired, and appealable, and private data belongs to each participant [14]. In order to solve the data security problems faced by the traditional APTS, it is necessary to protect the privacy of participants in the whole agricultural product industry chain, based on safe and reliable data sharing, improve the enthusiasm of agricultural industrial organizations to participate in the construction and application of traceability system, and strengthen the effective supervision of regulatory agencies, enhancing consumers' confidence and satisfaction with the traceability results. Hyperledger blockchain is committed to providing new solutions for data security and privacy protection [15, 16]. For example, Hyperledger fabric has been used in the pharmaceutical traceability system [12]. The APTS fully meets the above characteristics, which is also the key application field of blockchain in agriculture.

Access control is the core key technology for data privacy protection. Through access permissions, data can only be accessed by the owner and authorized legal users. At present, the Permissioned Blockchain mainly adopts technologies such as organization (user) identity authentication, privacy channel, main/subchain data isolation [17], multi-subchain model [18, 19], endorsement strategy, transaction encryption, smart contract encryption, and privacy data set to realize access control of block data. Organizational identity authentication solves the access control problem at the blockchain network level and prevents unauthorized users from entering the blockchain network; the privacy channel realizes the logical isolation between the organizations inside and outside the channel and achieves access control at the channel level, but it has different circumstances, creating a separate privacy channel that will incur additional management overhead (such as maintaining chain code version, policy and Membership Service Provider (MSP)). Obviously, the main/subchain data isolation and multichain model also have the same kind of problems as mentioned above, and endorsement policy can realize the organizational level access control of smart contract writing, but there is a risk of privacy disclosure due to cross-channel unauthorized access, and transaction encryption and smart contract encryption mechanisms still remain at the channel level; privacy dataset can realize access control of privacy data without creating a new privacy channel, but it still stays at the organizational level.

None of the above technologies can achieve more fine-grained (such as organization-level/node-level) access control to meet the complex access requirements of the Permissioned blockchain across organizations [20], and other access control technologies are still needed. Fabric CA 1.4 version has adopted Attributes-based Access Control (ABAC), through the organization of identity attributes to access control of smart contract (chain code) operations, but it still lacks flexibility to set attributes only from the perspective of organizational identity. At the same time, the confidentiality of shared data cannot be guaranteed. Wang et al. [21] proposed an Attribute-based Distributed Access Control Framework (ADAC) suitable for IoT blockchain. Based on ABAC and blockchain, Zhang et al. [22] use the access tree [23] to configure access policies to achieve fine-grained authorized access to IoT devices. ABE is also used for access control of data sharing under the blockchain. Alniamy and Taylor [24] proposed fine-grained access control of shared data under the distributed environment of the blockchain. Jemel and Serhrouchni [25] and Huang et al. [26] solved the problem of fine-grained access control faced by data protection in an open shared environment, but the attribute set is open to all nodes in the entire network, which can easily be stolen by malicious nodes to generate correct users Key. Wang et al. [20] used ABE to propose a data access control and sharing model to achieve fine-grained access control and secure sharing. With the increasing number of on-chain organizations, when cross-organization deployment increases information sharing between different organizations, ABAC implementation may become complicated and requires attribute management infrastructure [27].

However, the above-mentioned existing research only focuses on the design of fine-grained access control and does not provide an overall plan that includes attribute management infrastructure and effective supervision of encrypted data, which is not conducive to the unified supervision of encrypted data by supervision organizations.

2.3. Block Data Encryption and Flexible Sharing. Use blockchain distributed ledger and encryption technology to realize the privacy protection and safe sharing of agricultural global data, so as to ensure the stability of agricultural system operation and ensure the business flow (information flow), capital flow, and logistics data of the entire agricultural industry chain authenticity [5]. Data confidentiality is a prerequisite to ensure data security. Block (ledger) data security mainly encrypts transaction data through cryptographic algorithms. Symmetric encryption system can be used for blockchain data encryption [20, 28]. This system requires both encryption and decryption parties to share keys. The ciphertext data can be calculated using a multikey fully homomorphic encryption (MFHE) scheme. Chen et al. proposed a dynamic multikey FHE scheme based on the LWE assumption [29], which requires less "local" memory, and the ciphertext expansion process is distributed. With the increasingly complex business exchanges between organizations and the dynamic changes in the number of organizations, key distribution and management will become complicated and difficult to operate. At the same time, there will be key leakage and multiple encryption problems. If the entire blockchain uses the same cryptographic algorithm and key, it is meaningless for data protection in the blockchain. What is more dangerous is that once an organization or node is illegally compromised, the loss is

immeasurable. Obviously, symmetric cryptosystem is not the best choice for blockchain data encryption.

Relatively speaking, a public key cryptosystem based on Public-Key Infrastructure (PKI) is more suitable. At present, blockchains mostly use public key cryptosystems to encrypt data [20]. Although they have high security, they are limited to data sharing between the two, which cannot meet the data sharing of 1-to-*N* and multilevel access control [20]. In order to support more flexible public key generation, Sahai and Waters [30] proposed an Attribute-based Encryption (ABE) scheme, which uses a series of attribute sets instead of unique identifiers to identify identities. ABE is a fine-grained 1-to-N encryption scheme. Its advantages are as follows:

(1) Encryption is only related to attributes, without paying attention to the number and identity of access members, which reduces the encryption overhead

(2) Only the members that conform to the ciphertext attribute can be decrypted, so as to ensure the security of the data

(3) The key is related to random numbers, and the keys of different members cannot be combined, which can resist collusion attacks [20]

Further research proposes Key-policy Attribute-based Encryption (KP-ABE) [31] and Ciphertext-policy Attribute-based Encryption (CP-ABE) [32]. KP-ABE embeds the policy into the encryption key and the attribute into the ciphertext. The key corresponds to an access structure and the ciphertext corresponds to a set of attributes. CP-ABE embeds the policy into the ciphertext and the attribute into the user key. The ciphertext corresponds to an access structure, and the key corresponds to a set of attributes. The common feature of the two is to bind data encryption and decryption with policy. The data can be decrypted only when the attributes in the attribute set can meet the access structure. While retaining the ciphertext control, fine-grained access control can be realized. KP-ABE scheme is close to static scenarios, such as paid video websites and log encryption management. In CP-ABE scheme, the data owner specifies the strategy of accessing ciphertext and associates the attribute set with the access resources. Data users can access ciphertext data according to their own attributes. This technology is suitable for access applications such as private data sharing, such as data encryption storage and fine-grained sharing in cloud computing environment.

In view of the above analysis, this paper uses CP-ABE scheme to encrypt the data stored in the APTS, which can not only protect the data privacy and security of the uplink organization, but also lay a foundation for flexible data sharing.

3. BCST-APTS: Secure and Trusted Agricultural Product Traceability System

3.1. System Logic Architecture. A secure and trusted agricultural product traceability system covers the entire process of production, processing, warehousing, logistics, and sales in the agricultural product supply chain. Participating entities include farmers/producers, processors, warehouse operators, logistics providers, retailers, and consumers. The business of each participant is carried out under the effective supervision of the Regulatory authority. The regulatory authority is responsible for the identity authentication, authority management, data supervision, and traceability of agricultural product quality and safety events for each subject. The system logic architecture is shown in Figure 1.

The system realizes the whole process data collection of agricultural products "from farm to table," that is, preproduction data, mid-production data, and postproduction data, including structured data and unstructured data. Structured data can be encrypted and stored directly on the blockchain, and unstructured data can be stored off blockchain, but its digital fingerprints must be stored on the blockchain to ensure the integrity and confidentiality of the data. Based on Permissioned blockchain and data encryption technology, the system has the following technical characteristics.

(1) *No Tampering*. Ensure the authenticity, validity, and permanence of data stored on the chain.

(2) *Distributed Storage*. Sharing by members of the whole blockchain avoids the technical risks of centralized architecture.

(3) *Data Encryption and Flexible Access Control*. It can protect the privacy of the data publisher and solve the problem of separation of data ownership and control on the blockchain.

(4) *Tracing Smart Contract*. When an agricultural product quality and safety incident occurs, the data of relevant participants can be automatically extracted and uploaded to the system, so as to prevent the relevant parties from tampering, deleting, or forging data when the incident occurs, so as to restore the truth of the incident and find the root cause of the problem.

In the above architecture, data encryption and flexible access control are the keys to ensuring that this system has the characteristics of security and credibility. It is also a typical difference between this work and other agricultural product traceability systems based on blockchain technology. In order to achieve the unification of the two, this paper focuses on the realization of the encryption and fine-grained access control of the data on the blockchain based on the CP-ABE scheme. The reencryption scheme based on ciphertext policy attribute encryption (RE-CP-ABE) is introduced in detail in Section 4.

3.2. System Deployment Network Architecture. As mentioned in Section 3.1, the BCST-APTS involves multiple participants in the agricultural product supply chain. At present, in order to achieve efficient management within the enterprise, each entity has built a relatively complete information system, but the business system of each entity has huge differences in business logic, technical architecture, and deployment plans. Therefore, so as to achieve various

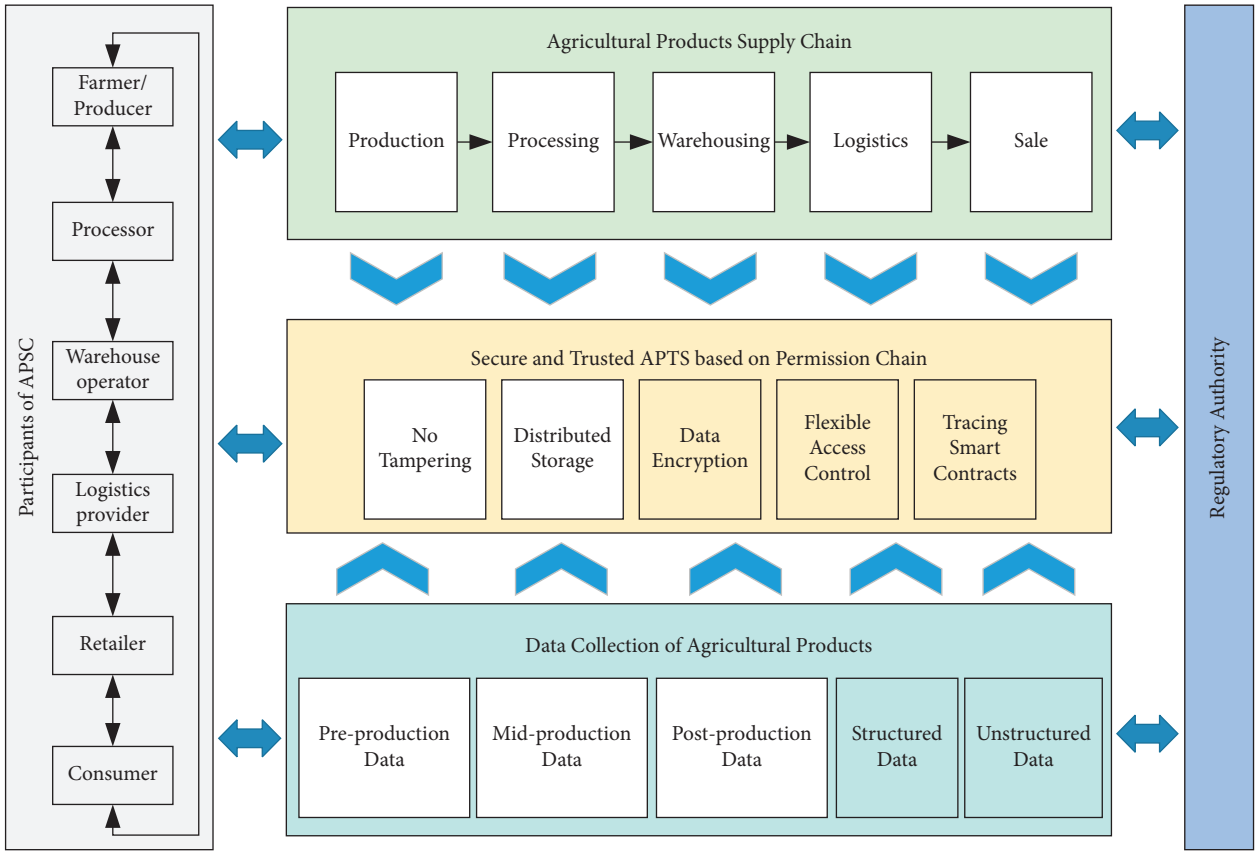

Figure 1: The system logic architecture of BCST-APTS.

business alliances, data sharing and business systems between subjects must solve the problems of multisource and heterogeneous internal business systems. The distributed characteristics of blockchain technology itself provide a new solution to the above problems. Figure 2 shows the deployment network architecture diagram of the system.

As shown in Figure 2, between the internal business system of each participant and the blockchain system, one or more blockchain nodes are built, and the internal business system and BCST-APTS are realized with the help of the client. For seamless connection of the blockchain, such as Organization A, Organization B, and Organization C as different participants in the agricultural product supply chain, there is also a regulatory organization responsible for supervision and operation of the entire blockchain system.

Note. The regulatory organization here is not a traditional centralized agency; it is just one of the ordinary members on the blockchain. When agricultural products need to be traded, the relevant data is packaged, and private data and trade secret data are encrypted using the CP-ABE encryption algorithm. The encrypted ciphertext is released and stored on the blockchain through the blockchain node, and data retrieval is only completed on the local blockchain node.

From the perspectives of part of the enterprise and the entire chain as a whole, the system architecture has obvious advantages. First of all, from the perspective of the organization, not only can the stability of the internal business system be ensured, but also a secure and reliable blockchain system can be accessed. Secondly, from the overall perspective of the entire chain, all participants jointly maintain a set of ledger books to achieve cross-regional and cross-industry agricultural product traceability business collaboration and data sharing, so as to ensure the authenticity and credibility of agricultural product traceability.

4. Reencryption Scheme Based on Ciphertext-Policy Attribute Encryption (RE-CP-ABE)

4.1. CP-ABE Scheme Features. The data in the blockchain ledger is open to the whole nodes, which cannot guarantee the confidentiality of the data and is easy to be accessed illegally. This paper introduces CP-ABE encryption scheme to ensure the data confidentiality and authorized access control of the data sharers and realize the unity of data ownership and control on the blockchain. CP-ABE Encryption Scheme [32] consists of five basic algorithms, including setup, encrypt, keygen, decrypt, and delegate. Among them, CT = encrypt (PK, m, t) is an encryption algorithm. The encryption algorithm encrypts a message m under the tree access structure T. The specific calculation formula is as follows:

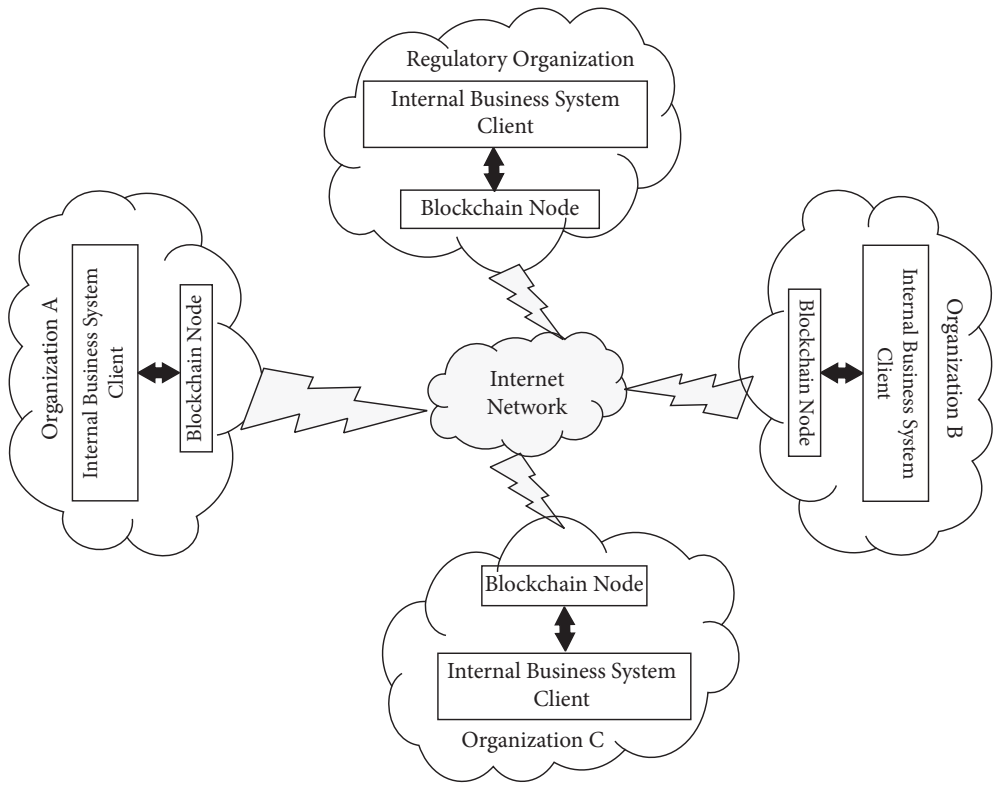

Figure 2: System deployment network architecture of BCST-APTS.

$$\mathrm{CT} = \left(T, \breve{C} = \mathrm{Me}(g,g)^{\alpha s}, C = h^{s}, \forall y \in Y: C_y = g^{q_y(0)}, C_y' = H(att(y))^{q_y(0)}\right). \tag{1}$$

Here, the ciphertext CT is constructed by T, which is the tree access structure. The function $att(x)$ is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in T.

The decryption function is DecryptNode (CT, SK, x), defined as

$$\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, \mathrm{x}) = \frac{e(D_i, C_x)}{e(D_i', C_x')} = \frac{e\left(g^{r} \cdot H(i)^{r_i}, h^{q_x(0)}\right)}{e\left(g^{r_i}, H(i)^{q_x(0)}\right)} = e(g,g)^{r q_x(0)}. \tag{2}$$

Here, SK is a private, which is associated with a set S of attributes, and a node x from T.

Reference [32] explains the meaning of other parameters in detail, which will not be repeated here. However, from the above two formulas and parameters T and $attr$ (x), it can be seen that, in CP-ABE algorithm, the attribute is extremely important for data encryption, decryption, and access control. It determines the flexibility of access control policy and who can decrypt ciphertext data. However, in order to meet the personalized encryption needs of each subject accessing the APTS, the system should support the needs of each subject to set personalized attributes, but it will lead to the increase of attribute synonymy or redundancy. At the same time, it is not conducive to the efficient supervision of encrypted data by regulators.

4.2. Access Control Tree. Figure 3 shows an access control tree model in Apple's traceability system. In order to show the principle, it only includes four parts: product type, brand, place of production, and logistics provider.

It can be seen from Figure 3 that leaf nodes represent an attribute of shared data, and non-leaf nodes are threshold nodes that support "AND" or "OR" logic operations. Data requesting organization must meet the minimum threshold value before they can decrypt the secret value of this node. For example, the threshold node "1/2" means that at least one of the two attributes can be decrypted, which is one of JD.com or SF Express. When the data requesting organization applies for access to encrypted data, only users who have the attributes in the access control tree and satisfy the logical relationship can access, so that the data can be encrypted once and shared N times.

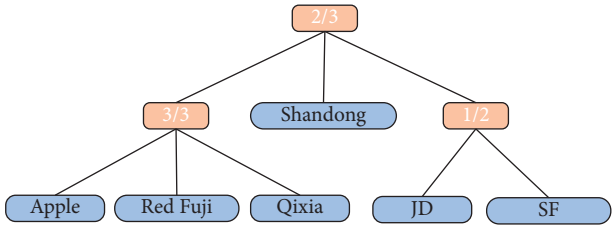

Figure 3: Access control tree model in Apple's traceability system.

4.3. Attribute Management Infrastructure. To solve the above-mentioned problems, this paper proposes that the authoritative organization or regulatory authority in the APTS builds a whole-chain standardized attribute management infrastructure to provide attribute management, access, and other services to all access organizations in the entire blockchain. The specific construction process of this attribute management infrastructure is shown in Figure 4.

The construction of the attribute management infrastructure includes the following steps:

(1) Initialization phase: at this stage, the authoritative organization establishes the structure and storage mode of the attribute management infrastructure and establishes the user attribute set to standardize the management of all attributes of the whole chain. The structure of attribute management infrastructure can adopt key value, relational table, etc., and be stored in the form of file or database table. The user attribute set is used to store all attribute sets owned by the organization.

(2) Assign public attributes to the access organization. When approving the access application of each organization, the authoritative organization assigns public attributes to the application organization according to its business, role, etc. The public attributes can be organization name, organization identity ID, system role, access time, and other different contents.

(3) The access organization applies for private attributes. After accessing the permissioned blockchain system, each organization can apply to an authoritative organization to maintain its own private attributes based on its own business development. The authoritative organization decides whether to approve the application. After passing the application, the organization can be used for subsequent data encryption and decryption.

(4) Establish a whole-chain attribute management infrastructure. The public and private attributes of each organization together constitute the entire blockchain of attribute management infrastructure.

(5) Maintain the attributes of the entire blockchain. The authoritative organization dynamically maintains and manages the attributes of the entire blockchain and the attribute collection in the attribute management infrastructure according to the result of the attribute application.

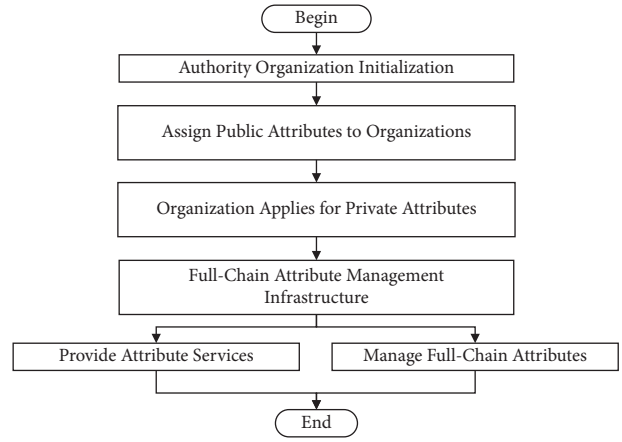

Figure 4: Flowchart of whole-chain attribute management infrastructure.

(6) Provide attribute services. Authoritative organizations provide external attributes services such as query, modification, and deletion according to the attribute management infrastructure and the attribute collection of the organization. For example, the data issuer retrieves the attributes used for data encryption, and when the authoritative organization works in place of the CA, it can generate encryption keys based on the data issuer.

The above attribute management infrastructure construction method manages the attributes of the entire blockchain through the attribute dictionary, which can not only meet the personalized attribute requirements of different access organizations, but also convert redundant attributes and synonymous attributes into standardized and standard attributes. A flexible and efficient solution is proposed for the difficult problem of attribute management in attribute-based encryption schemes.

4.4. RE-CP-ABE Encryption Scheme. The CP-ABE encryption scheme can configure flexible and personalized encryption and access control policies with the help of attributes, but it also poses challenges for the entire blockchain of sharing and supervision of encrypted data. When the data issuer releases the encrypted data to the traceability system, if the original access control policy remains unchanged, it can be unified to the entire blockchain of standardized data encryption, so that the data owner, data requester, and data supervisors can quickly access data, which will greatly improve the management efficiency of the system. For this reason, RE-CP-ABE is proposed in this paper.

RE-CP-ABE scheme consists of six core algorithms: Setup, Encrypt, UpBlockChain , ReEncrypt, AccessKeyGen, and Decrypt. All variable symbols used in the specific algorithm are shown in Table 1.

$$\text{Setup}(\,) \longrightarrow \text{PK, MK.} \tag{3}$$

Table 1: Symbolic variable.

Variable name	Meaning
Setup	System initialization algorithm
PK	Public parameters
MK	Master key
Encrypt	Personalized encryption algorithm
M	Plaintext message
T	Personalized access control tree
CT	Personalized ciphertext
UpBlockChain	Block publishing algorithm
ReEncrypt	Attribute re-encryption algorithm
CT′	Standardized ciphertext
T'	Standardized access control tree
AccessKeyGen	Access control and key generation algorithm
S	Personalized attribute set selected by the data request user
SK	Decryption private key
Decrypt	Data decryption algorithm

System initialization algorithm: it has no input parameters, output public parameters PK, and master key MK.

$$\text{Encrypt}(\text{PK}, M, T) \longrightarrow \text{CT}. \tag{4}$$

Personalized encryption algorithm: according to the personalized access control tree T, it is constructed by users according to their own personalized needs, flexibly selected attribute set U_p and logical relations, and personalized encryption is performed on the plaintext message M to obtain a personalized ciphertext CT.

$$\text{UpBlockChain}(\text{CT}, T). \tag{5}$$

Block publishing algorithm. Publish the encrypted personalized ciphertext CT and the corresponding access control tree T to the authoritative organization node or block generation node of the blockchain system, such as the Orderer node of Fabric.

$$\text{ReEncrypt}(\text{PK}, \text{CT}, T) \longrightarrow \text{CT}', T'. \tag{6}$$

Attribute reencryption algorithm: this algorithm is executed by an authoritative organization node and uses the attribute service provided by the attribute management infrastructure to reencrypt the received personalized ciphertext CT into a standardized ciphertext CT′. At the same time, the personalized access control tree T is converted into a standardized access control tree T'.

$$\text{AccessKeyGen}(T', S) \longrightarrow \text{SK}. \tag{7}$$

Access control and key generation algorithm: the algorithm is executed by the authoritative organization node and uses the attribute service provided by the attribute management infrastructure to determine whether the personalized attribute set S selected by the data request user meets the standardized access control tree T'. If both the attributes and the logical relationship meet the requirements, the user's data decryption private key SK is generated. Otherwise, there is no access control authority, and the decryption private key SK cannot be obtained.

$$\text{Decrypt}(\text{PK}, \text{CT}', \text{SK}) \longrightarrow M. \tag{8}$$

Data decryption algorithm: according to the system public parameter PK and the decryption private key SK, the standardized data ciphertext CT′ is decrypted into plaintext message M.

This algorithm is an improvement of the CP-ABE [32] scheme and retains the technical advantages of the original algorithm that flexibly set access control policies and data encryption according to attributes. At the same time, with the help of a standardized access control tree T', it is possible to realize the standardization of personalized data encryption and access control, so that access rights can be quickly determined, and the effective supervision of encrypted data by data supervision organizations and authoritative third parties can be ensured.

5. BCST-APTS Based on Fabric and RE-CP-ABE

5.1. BCST-APTS Scheme. As one of the typical representatives of the Permissioned Blockchain, the fabric has been widely studied and applied in various fields. It realizes the technical positioning of business collaboration for alliance members, which determines that it can be successfully applied to the traceability system of agricultural products. This paper designs a secure and trusted agricultural product traceability system scheme based on Fabric and RE-CP-ABE, as shown in Figure 5.

This system scheme consists of data publisher (Organization 1), data requester (Organization N), and authoritative organizations, and the authoritative organization is responsible for the operation and maintenance management of the CA node and Orderer node of the system. Each connected organization manages its own Peer node and saves a copy of the blockchain ledger with the entire chain data.

5.2. Business Process. The specific business process of the scheme is as follows:

(1) Data is encrypted and published on the blockchain. The data publisher (organization 1) uses the

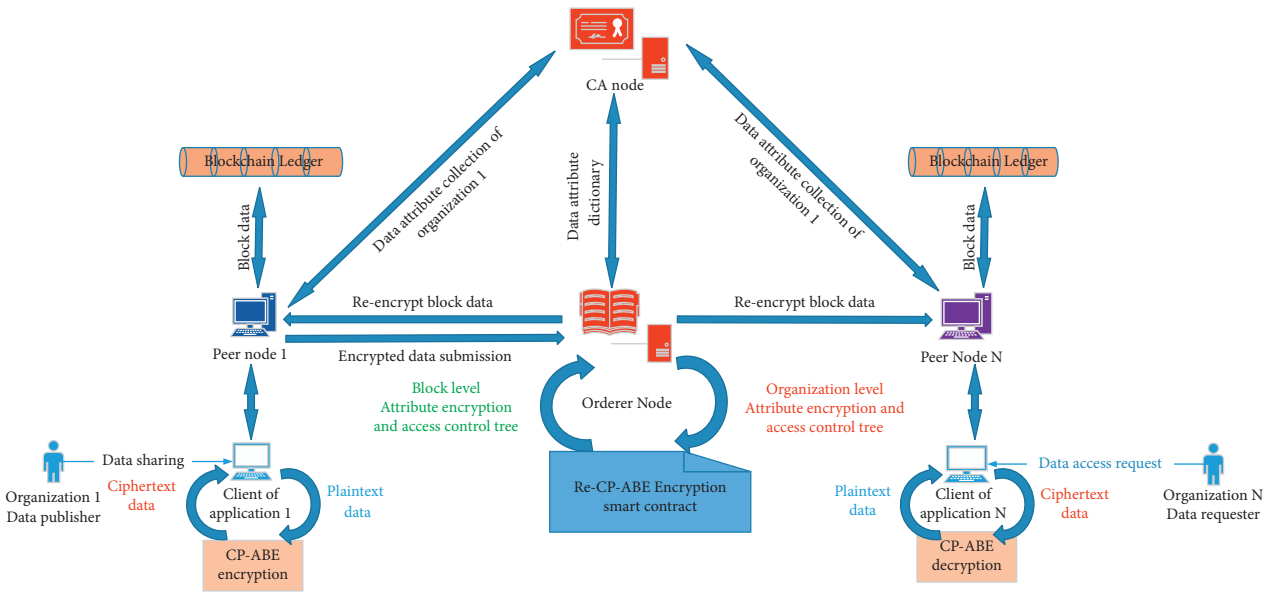

Figure 5: BCST-APTS scheme based on fabric and RE-CP-ABE.

application 1 client to interact with Peer node 1, which is a node managed by itself, for blockchain interaction. The client is responsible for selecting attributes for encryption and constructing an access tree. After attribute encryption, the ciphertext data is submitted to the Peer node for publishing on the blockchain.

(2) Reencryption by authoritative organizations: the RE-CP-ABE encrypted smart contract is deployed in the Orderer node, and the Orderer node uses it to reconstruct the access tree of shared data, that is, converting it to the canonical access tree under the attribute dictionary, and reencrypting the data. As a result, the ciphertext data (organization level) encrypted by different organization attributes is converted to the ciphertext data (block level) under the specification attributes of the whole-chain attribute dictionary.

(3) Store standard ciphertext data blocks: the Orderer node is responsible for sorting the received transactions, generating blocks of reencrypted data, broadcasting them to each Peer node 1 and Peer node N on the permissioned blockchain, and writing them into the blockchain ledger.

(4) The data requester decrypts: the data requester (organization N) sends the data request and the attributes it owns to the Peer node N through the client of the application N. Then, the Peer node N automatically executes the smart contract constructed by the canonical access tree to check whether the attributes and access control of data access are met condition. If it is determined to be satisfied, it returns to the client a request response including encrypted data and a standardized access control tree. The application N client decrypts the returned encrypted data to obtain the plaintext data.

5.3. Security Analysis. In the proposed scheme, the CP-ABE encryption algorithm is used to protect data privacy and access control, the blockchain technology is used to ensure the distributed storage of data, and the RE-CP-ABE scheme is designed to ensure efficient data supervision of encrypted data to ensure the security and efficiency of the design scheme.

(1) Data confidentiality: this solution uses CP-ABE to encrypt the data on the blockchain and stores the ciphertext data on the blockchain. Although all nodes of the blockchain can obtain the data, the data content cannot be obtained when the attributes and access control tree requirements are not met. Therefore, data privacy and security are protected.

(2) Data integrity: this solution stores the traceability data of agricultural products on the blockchain. With the help of the chain storage structure of the blockchain ledger, it can effectively prevent a single node from tampering with the data and ensure the integrity of the traceability data.

(3) Data availability: all nodes participating in the traceability system can have a copy of the complete ledger. Therefore, when the service of a single node or multiple nodes is abnormal or interrupted, the entire system can still operate normally, which can effectively guarantee the availability of the system and data.

(4) Binding security of data ownership and control rights: taking full advantage of the fine-grained access control technology of the CP-ABE algorithm, it solves the problem of the data owner's control of distributed storage data on the blockchain and, at the same time, realizes one-time encryption for data release and multiple authorizations for data access, thereby improving the security and flexible access flexibility of the data on the blockchain.

(5) Reencryption security: the RE-CP-ABE scheme designed in this paper is implemented by the Orderer node of an authoritative organization, which can effectively identify malicious attribute operations such as forgery and impersonation by participants, thereby further ensuring the security of reencrypted data.

6. Conclusion and Prospect

In this paper, blockchain technology and CP-ABE algorithm are successfully integrated and applied to a secure and trusted agricultural product traceability system (BCST-APTS). Furthermore, an attribute management infrastructure is designed, which can regulate and efficiently manage the attributes of the entire blockchain. Based on this and CP-ABE algorithm, a RE-CP-ABE scheme is proposed, which can convert personalized encryption to standardized encryption, thereby ensuring the efficient sharing and supervision of data stored in the Permissioned Blockchain. Finally, this paper designs a BCST-APTS scheme based on Fabric and RE-CP-ABE. The above research work provides new solutions and ideas for solving the problems of data fraud, untrustworthy traceability results, and privacy leakage in the APTS. This work currently only designs the model of the system from the perspective of technology, architecture, and principles. The follow-up will focus on an in-depth research on the security of smart contracts, the efficiency of attribute management infrastructure, the flexibility and efficiency of the RE-CP-ABE solution, and the final construction a complete and usable APTS serving the development of agricultural product traceability technology.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors did not have any conflicts of interest.

Acknowledgments

This work was supported by the Project of Shandong Provincial Natural Science Foundation under Grant no. ZR2021QF056, National Natural Science Foundation of China under Grant nos. 62071320 and 61771090, Tai'an Science and Technology Innovation Development Project under Grant no. 2020NS080, and Shandong Federation of Social Sciences under Grant no. 2021-YYGL-32.

References

[1] S. C. Graves, D. B. Kletter, and W. B. Hetzel, "A dynamic model for requirements planning with application to supply chain optimization," *Operations Research*, vol. 46, pp. 35–49, 1998.

[2] G. P. Cachon and M. Fisher, "Supply chain inventory management and the value of shared information," *Management Science*, vol. 46, no. 8, pp. 1032–1048, 2000.

[3] M. Boehlje, J. Akridge, and D. Downey, "Restructuring agribusiness for the 21st century," *Agribusiness*, vol. 11, no. 6, pp. 493–500, 1995.

[4] J. Gao, J. Teng, L. Hou, and X. Liu, "Pricing strategy of closed-loop supply chain considering competition under uncertain demand," *Journal of Systems Engineering*, vol. 32, pp. 78–88, 2017, in Chinese.

[5] W. Gao, G. Zhang, G. Zhang et al., "Original innovation of key technologies leading healthy development of smart agricultural," *Smart Agriculture*, vol. 1, no. 1, pp. 8–19, 2019, in Chinese.

[6] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, "Semi-selfish mining based on hidden Markov decision process," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3596–3612, 2021.

[7] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, pp. 1–22, 2021.

[8] J. Liu, T. Yang, and W. Wang, "Traceability system using public and private blockchain," *Journal of Cyber Security*, vol. 3, no. 3, pp. 17–29, 2018, in Chinese.

[9] T. Feng, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, Kunming, China, June 2016.

[10] X. Yang, M. Wang, D. Xu, N. Luo, and C. Sun, "Data storage and query method of agricultural products traceability information based on blockchain," *Transactions of the Chinese Society of Agricultural Engineering*, vol. 35, no. 22, pp. 323–330, 2019, (in Chinese).

[11] J. Zhu, Q. Ding, and S. Gao, "Distributed Framework of SWIFT system based on permissioned blockchain," *Journal of Software*, vol. 30, no. 6, pp. 1594–1613, 2019, (in Chinese).

[12] M. Uddin, "Blockchain Medledger: hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, Article ID 120235, 2021.

[13] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs," *International Journal of Intelligent Systems*, 2021.

[14] L. Yu, G. Zhang, J. Jia, and W. Gao, "Modern agricultural product supply chain based on block chain technology," *Transactions of the Chinese Society for Agricultural Machinery*, vol. 48, pp. 387–393, 2017.

[15] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, "The revolution of blockchain: state-of-the-art and research challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1497–1515, 2020.

[16] A. A. Khan, M. Uddin, A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 99, 2021.

[17] X. Min, Q. Li, J. Kong, and D. Zhang, "Permissioned blockchain dynamic consensus mechanism based multi-centers," *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 41, no. 5, pp. 1005–1020, 2018, (in Chinese).

[18] Q. Ding, J. Zhu, J. Zhang et al., "Traceability permissioned chain consensus mechanism based on double-layer architecture," *Journal of Network and Information Security*, vol. 5, no. 2, pp. 1–12, 2019, (in Chinese).

[19] W. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in *Proceedings of the 2016 IEEE*

Symposium on Service-Oriented System Engineering (SOSE), April 2016.

[20] X. Wang, X. Jiang, and Y. Li, "Model for data access control and sharing based on blockchain," *Ruan Jian Xue Bao/Journal of Software*, vol. 30, no. 6, pp. 1661–1669, 2019, (in Chinese).

[21] P. Wang, Y. Yue, W. Sun, and J. Liu, "An attribute-based distributed access control for blockchain-enabled IoT," *Networking and Communications (WiMob)*, in *Proceedings of the 2019 International Conference on Wireless and Mobile Computing*, pp. 1–6, Barcelona, Spain, October 2019.

[22] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics*, vol. 9, no. 2, p. 285, 2020.

[23] A. Castiglione, A. Santis, B. Masucci et al., "Hierarchical and shared access control," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 850–865, 2016.

[24] A. Alniamy and B. D. Taylor, "Attribute-based access control of data sharing based on hyperledger blockchain," in *Proceedings of the ICBCT'20: 2020 The 2nd International Conference on Blockchain Technology*, pp. 135–139, Hilo, HI, USA, March 2020.

[25] M. Jemel and A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in *Proceedings of the IEEE International Conference on E-business Engineering IEEE*, pp. 177–182, Shanghai, China, November 2017.

[26] S. Huang, W. Chen, and B. Fan, "Data security sharing method based on CP-ABE and blockchain," *Computer Systems & Applications*, vol. 28, no. 11, pp. 79–86, 2019.

[27] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[28] Z. Huang, "The application of blockchain in edge computing and IoT," *Cyberspace Security*, vol. 9, no. 8, pp. 25–30, 2018.

[29] Y. Chen, S. Dong, T. Li, Y. Wang, and H. Zhou, "Dynamic multi-key FHE in asymmetric key setting from LWE," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5239–5249, 2021.

[30] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Lecture Notes in Computer Science*, in *Proceedings of the International Conference on Theory & Applications of Cryptographic Techniques*, pp. 457–473, Aarhus, Denmark, May 2005.

[31] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, Alexandria Virginia, USA, October 2006.

[32] J Bethencourt, A. Sahai, and B Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security & Privacy*, pp. 321–334, IEEE, Berkeley, CA, USA, May 2007.