scientific reports

Check for updates

OPEN

Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products

Shaohua Wang[1,2], Na Luo[1,3], Bin Xing[1,3], Zhenzhen Sun[1,2], Hang Zhang[2,4]✉ & Chuanheng Sun[1,2,4]✉

In today's globalized agricultural system, information leakage of agricultural biological risk factors can lead to business risks and public panic, jeopardizing corporate reputation. To solve the above problems, this study constructs a blockchain network for agricultural product biological risk traceability based on agricultural product biological risk factor data to achieve traceability of biological risk traceability data of agricultural product supply chain to meet the sustainability challenges. To guarantee the secure and flexible sharing of agricultural product biological risk privacy information and limit the scope of privacy information dissemination, the blockchain-based proxy re-encryption access control method (BBPR-AC) is designed. Aiming at the problems of proxy re-encryption technology, such as the third-party agent being prone to evil, the authorization judgment being cumbersome, and the authorization process not automated, we design the proxy re-encryption access control mechanism based on the traceability of agricultural products' biological risk factors. Designing an attribute-based access control (ABAC) mechanism based on the traceability blockchain for agricultural products involves defining the attributes of each link in the agricultural supply chain, formulating policies, and evaluating and executing these policies, deployed in the blockchain system in the form of smart contracts. This approach achieves decentralization of authorization and automation of authority judgment. By analyzing the data characteristics within the agricultural product supply chain to avoid the malicious behavior of third-party agents, the decentralized blockchain system acts as a trusted third-party agent, and the proxy re-encryption is combined with symmetric encryption to improve the encryption efficiency. This ensures a efficient encryption process, making the system safe, transparent, and efficient. Finally, a prototype blockchain system for traceability of agricultural biological risk factors is built based on Hyperledger Fabric to verify this research method's reliability, security, and efficiency. The experimental results show that this research scheme's initial encryption, re-encryption, and decryption sessions exhibit lower computational overheads than traditional encryption methods. When the number of policies and the number of requests in the access control session is 100, the policy query latency is less than 400 ms, the request-response latency is slightly more than 360ms, and the data uploading throughput is 48.7 tx/s. The data query throughput is 81.8 tx/s, the system performance consumption is low and can meet the biological risk privacy protection needs of the agricultural supply chain. The BBPR-AC method proposed in this study provides ideas for achieving refined traceability management in the agricultural supply chain and promoting digital transformation in the agricultural industry.

Keywords Agricultural products biological risk factors, Privacy protection, Blockchain, Re-encryption, Attribute based access control

[1]National Engineering Laboratory for Agri-product Quality Traceability, Beijing 100097, China. [2]College of Computer and Information Engineering, Tianjin Agriculture University, Tianjin 300384, China. [3]National Engineering Research Center for Information Technology in Agriculture, Beijing 100097, China. [4]These authors contributed equally: Hang Zhang and Chuanheng Sun. ✉email: zhangh@tjau.edu.cn; sunch@nercita.org.cn

In modern agricultural production, the traceability of agricultural biological risks has become one of the focuses of attention. Agricultural biological risk factors are biological factors that may affect the safety and quality of agricultural products, including pathogenic microorganisms, fungal toxins, pests and their pest-borne pathogens, insect residues, and genetically modified organisms[1]. These factors may lead to contamination or deterioration of the quality of agricultural products, posing a potential hazard to human health[2]. Failure to monitor and control these biological risk factors promptly in the supply chain of agricultural products may result in a chain reaction that affects consumer health and the sustainable development of the industry[3]. The transmission pathways of agricultural biological risk factors are shown in Fig. 1.

In recent years, there has been a high incidence of food safety incidents in China due to foodborne biological risk factors in agricultural products[4]. As shown in Fig. 2a, Food safety incidents due to foodborne biological risk factors in China climbed yearly from 2011 to 2020; As shown in Fig. 2b, Food safety incidents due to foodborne biological risk factors occur mainly in the food service sector as well as in households; As shown in Fig. 2c Animals, plants and poisonous mushrooms and other causes predominate among food safety incidents due to various foodborne biological risk factors; As shown in Fig. 2d, vegetables, mushrooms, aquatic products and meat in agricultural products accounted for the major portion of food safety incidents due to foodborne biological risk factors in various categories[5].

Therefore, the establishment of a full-process traceability system for biological risk factors of agricultural products can improve market transparency, enhance consumer trust, and promote trade development. Based on existing research, a biological risk factor prevention level is established, and through the traceability system, regulatory agencies and enterprises can discover and investigate potential sources of contamination promptly, reduce the probability of food safety accidents, safeguard public health, realize the organic connection between the safe production and consumption of agricultural products, and promote the sustainable development of agriculture.

Blockchain technology is a distributed, decentralized ledger technology that ensures the security and trustworthiness of data through cryptography and consensus algorithms[6]. Blockchain technology links data in the form of blocks to form an immutable record, achieving transparency and traceability of information, and providing a secure and trustworthy interaction environment for all participants. As an interdisciplinary and innovative technology, blockchain technology has important advantages in enhancing the traceability of biological risk factors in the agricultural supply chain. Its decentralized nature eliminates the problem of centralized storage of biological risk factor information and ensures the integrity and security of the information; its tamper-resistant

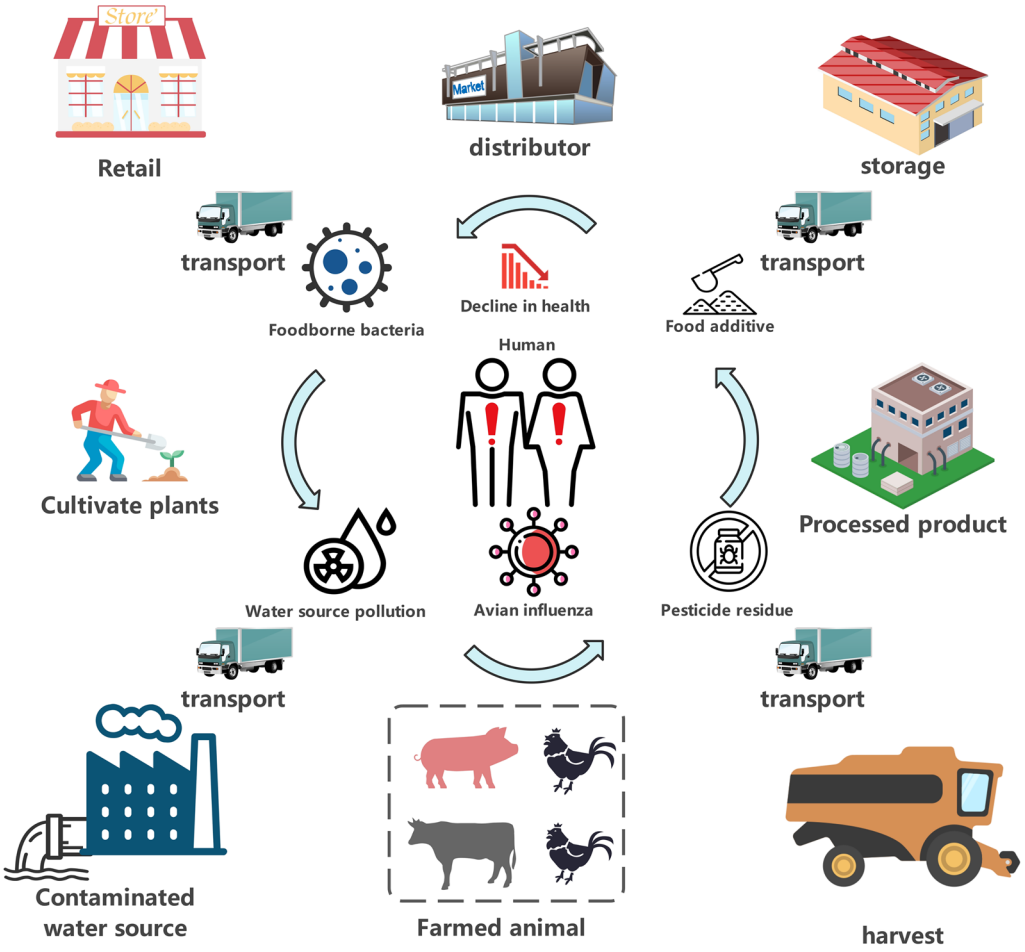


Fig. 1. Transmission route of biological risk factors of agricultural products.

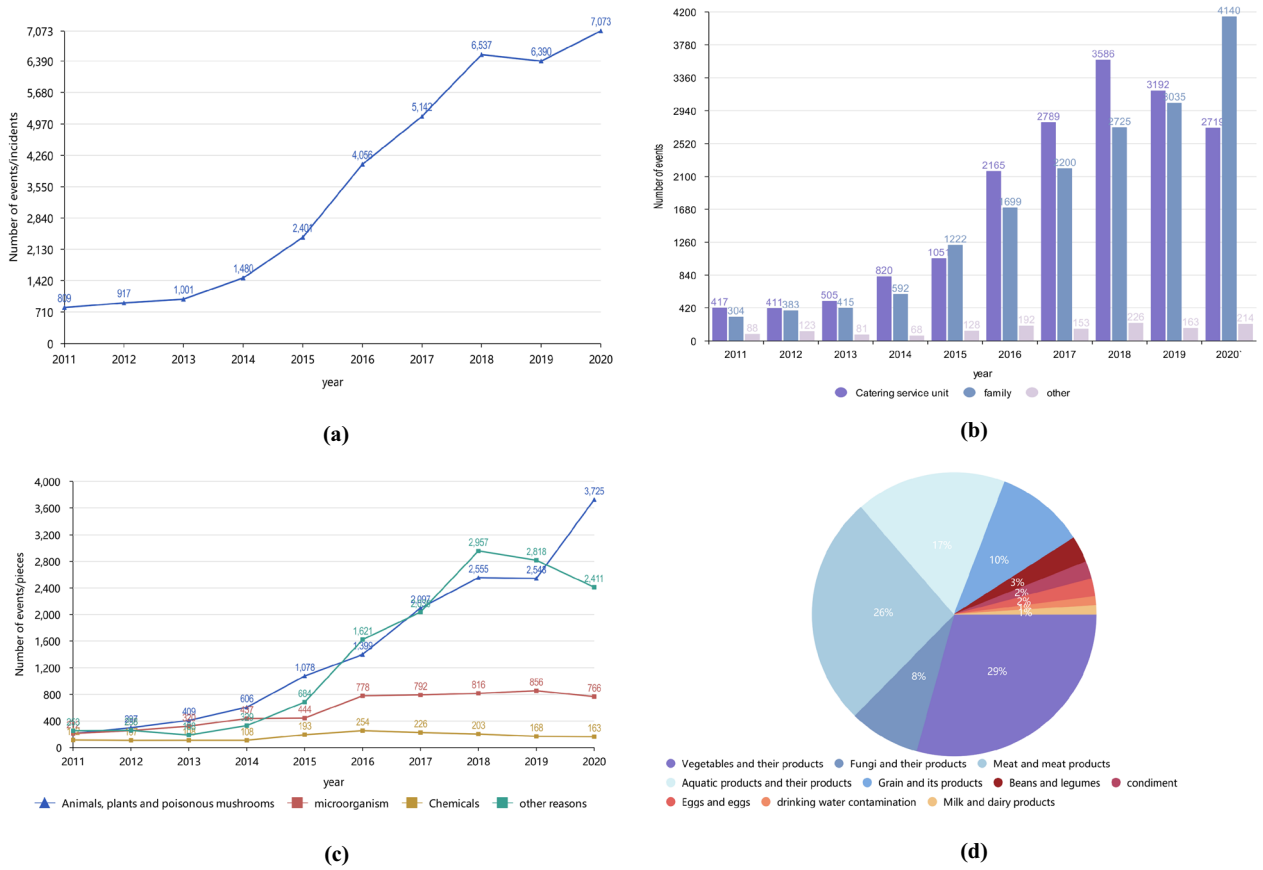


Fig. 2. Incidence of food-borne biological risk factors in China in recent years. (**a**) Number of foodborne disease outbreaks in China, 2011-2020 (**b**) Number of foodborne disease outbreaks at different sites in China, 2011-2020 (**c**) Number of foodborne disease outbreaks caused by different causative factors in China, 2011-2020 (**d**) Food Categories Involved in Food Poisoning Incidents.

nature solves the problem of easy tampering of the risk factor information and ensures the authenticity and credibility of the information; and its transparency meets the needs of the regulatory bodies for the transparency of biological risk factor information in the supply chain[7].

The special nature of agricultural biological risk factor information lies in its key role in the supply chain. Information leakage may lead to the disclosure of trade secrets, triggering unfair competition and economic losses. In addition, malicious use of such information may increase food safety risks, reduce food quality, or even lead to contamination and endanger public health. Public perceptions of biological risk factors in agricultural products may trigger consumer panic, reduce trust in the company, affect sales, damage the company's reputation, and even trigger a crisis of confidence in the industry. Therefore, strengthening agricultural risk management and data security can help avoid agricultural safety risks, safeguard individual rights and commercial interests, ensure data security and compliance, and promote the sustainable development of smart agriculture[8].

Privacy protection technology is a technological tool used to protect an individual's sensitive information from malicious access or disclosure. In blockchain traceability systems, the use of privacy-preserving technologies can effectively protect the privacy of participants while maintaining data traceability and integrity. Proxy re-encryption technology, as a privacy protection technology, is of great significance in the application of blockchain systems. By encrypting the data and delegating the operation to a third party, it achieves the protection of the data and the hiding of privacy, and at the same time ensures the security of data verification and transmission in the blockchain[9]. The use of proxy-heavy encryption technology not only improves the level of privacy protection but also effectively solves the contradiction between data sharing and privacy protection in the blockchain system, providing more possibilities for the expansion of blockchain applications[10].

Currently, there is less research on blockchain technology for agricultural product biological risk privacy protection. How to effectively protect the private information of agricultural biological risk under the premise of ensuring the efficient traceability of agricultural biological risk factors, timely blocking the circulation channels of problematic products, and improving the security of the agricultural supply chain has become an urgent research direction. Based on the above issues, this study designs a blockchain-based proxy re-encryption access control privacy protection method in the context of biological risk factor traceability of agricultural products, BBPR-AC enables the secure sharing of private information on biological risk factors for agricultural products. This will help improve regulatory efficiency, reduce costs, and achieve accurate regulation and rapid early warning. At the same time, it will help establish a transparent regulatory system, enhance public trust, promote the

safety of agricultural products and the stable development of markets, and lay the foundation for the sustainable development of the agricultural industry chain.

Contribution

The main contributions of this study are as follows:

1. The data of biological risk factors in the agricultural supply chain were analyzed, and the privacy levels of these factors were classified. A proxy re-encryption access control method based on blockchain was designed to address this. To mitigate the risk of malicious actions by third-party agents, the agricultural products traceability blockchain system is employed as a third-party agent to achieve decentralized re-encryption. Symmetric encryption is incorporated into this method to ensure the symmetric encryption of biological risk data, thereby enhancing encryption efficiency. An ABAC (Attribute-Based Access Control) mechanism tailored to the agricultural supply chain was developed, the relevant functions are implemented through smart contracts and deployed in the agricultural product traceability blockchain network. By defining the enterprise attribute information within the agricultural supply chain, the attribute management point disseminates this information, while the policy management point formulates policies for accessing biological risk factor data. The authorization process is automated and decentralized through the policy decision point and the policy execution point.
2. A blockchain network geared towards agricultural biological risk traceability was designed to write publicly available data on agricultural supply chain biological risks into the blockchain network to ensure regulatory traceability to address sustainability challenges.
3. A prototype blockchain system for agricultural biological risk traceability is built based on the Hyperledger Fabric platform, A blockchain browser has been developed to enhance the visualization of data within the agricultural product traceability system, the traceability process of agricultural biological risk factors is implemented, a biological risk factor detection report of agricultural products was designed as private data and the BBPR-AC access control method proposed in this study is realized through simulation experiments. Finally, the reliability, safety, and efficiency of the method proposed in this study are assessed by analyzing the performance indicators obtained from the experimental tests.

Chapter arrangement

The rest of the paper is organized as follows. Section "Related work" is a brief review of recent research in the areas and technologies involved in this study. Section "Blockchain-based proxy re-encryption access control method" analyzes the data on biological risk factors of agricultural products, introduces the design of the traceability information model of biological risk factors of agricultural products, and describes the design and workflow of each part of BBPR-AC. In section "Experimental test and results", the experimentally constructed blockchain network as well as the simulation experiments of the method proposed in this study, and the testing of related key performance indicators are presented, describing the test results. In section "Conclusions", a summary and outlook for this research is provided.

Related work

Risk traceability

Currently, blockchain technology is increasingly being researched and applied in the field of agricultural risk traceability. Researchers and practitioners have begun exploring the use of blockchain technology for supply chain management, product tracking, and information transparency. Biological risk sensors can obtain direct monitoring data[11], and blockchain technology can ensure that the acquired data is not tampered with, various participants, such as producers, processors, transporters, and consumers, can share and verify information on the production, processing, and transport of products, and realize full risk traceability. At the same time, the smart contract function of the blockchain is also capable of automatically enforcing the terms of the contract, ensuring that the participants comply with the agreed rules, and improving the transparency and reliability of risk factor traceability. Some studies have also explored how the Internet of Things (IoT) technology and blockchain technology can be combined to enable real-time monitoring and recording of product data such as temperature, humidity, and transport routes to further improve the accuracy and reliability of traceability systems[12]. In addition, there is research dedicated to addressing aspects such as scalability and efficiency of blockchain technology in food traceability, to better adapt to large-scale real-world application scenarios. Blockchain technology is also widely used in other fields, such as the safety traceability of drugs[13] and vaccines in the medical field. Mishra et al.[14] introduced "VaccineChain", a scalable blockchain secure vaccine supply chain model based on checkpoint assistance, which ensured the infeasibility of VaccineChain's calculation through comprehensive security analysis and standard theoretical proof. This also indirectly proves the applicability and security of blockchain technology in different industries.

Li et al.[15] took the testing data related to agricultural product quality and safety as the research object, sorted out the supply chain and business process of agricultural products, analyzed the risk factors of agricultural products under the influence of heavy metals, and established the risk evaluation model of agricultural product quality and safety. Salah et al.[16] propose a method for efficiently executing business transactions using Ethernet blockchain and smart contracts to enable soybean risk tracking and traceability throughout the agricultural supply chain. Alshehri et al.[17] created the Intelligent Livestock Farming System (IoT-BC-SLF) using blockchain technology. The framework incorporates IoT technology and allows for transparent and secure communication between farmers. Khanna et al., have proposed a blockchain-based supply chain platform for the dairy industry. The platform ensures the security and traceability of dairy products throughout the supply chain, thereby

preventing their customers from consuming counterfeit products and reducing the risk in the flow of dairy products[18]. Peng et al.[19] constructed a dynamic regulatory model framework based on blockchain and smart contracts to realize real-time management of the rice supply chain in terms of business information, hazard source information, and personnel information.

Privacy protection

Currently, there is a lack of research and application of blockchain technology and privacy protection technology in the field of agricultural products biological risk privacy protection, and relying on blockchain networks alone cannot solve the problem of secure sharing of biological risk privacy information. Yao et al.[20] proposed a trusted agricultural product traceability system based on the Ethernet blockchain. A dual storage model of "blockchain + IPFS (Interplanetary File System)" was designed to reduce the storage pressure of blockchain, and a data privacy protection solution based on cryptographic primitives and Merkle trees was proposed. Guan et al.[21] proposed a blockchain-based agricultural product traceability system model and designed a multi-channel data collection and uploading architecture to meet the actual traceability needs of various agricultural products. A layered encryption algorithm is used to encrypt the agricultural product information uploaded from each channel to achieve secure sharing of agricultural product information.

Traditional privacy protection algorithms are primarily categorized into symmetric encryption, asymmetric encryption, and a combination of both[10]. Symmetric encryption algorithms, such as AES, are renowned for their high encryption and decryption speeds and low computational resource consumption, making them suitable for large-scale data encryption. However, they pose challenges in key management and carry a high risk of key leakage. Asymmetric encryption algorithms, like RSA, simplify key management and enhance security through the use of paired public and private keys. Despite these advantages, their high computational complexity and slow processing speeds render them unsuitable for encrypting large volumes of data[22]. The hybrid encryption approach, which combines symmetric and asymmetric encryption, leverages the strengths of both methods. It uses asymmetric encryption to securely transmit symmetric keys, which are then used for data encryption, thereby enhancing security and maintaining efficiency. This method is extensively employed in SSL/TLS protocols to ensure secure and efficient network communication[23]. Nonetheless, hybrid encryption necessitates the management of both symmetric and asymmetric keys, increasing the complexity of implementation and maintenance.

Proxy re-encryption

Proxy re-encryption is an encryption method for delegated data access control that allows data holders to delegate encrypted data to others, authorizing them to decrypt and access specific portions of the data, while protecting individual privacy and ensuring data security and trustworthiness. In the traceability blockchain system, proxy re-encryption technology can achieve fine-grained access control, dynamically adjust the access rights to the data, improve the flexibility and security of data sharing, reduce the risks in the process of data transmission and storage, prevent data leakage and tampering, and enhance the traceability and integrity of the data. The application of agent-heavy encryption technology in the field of agricultural product traceability brings important technical advantages and guarantees for data security, privacy protection, and the credibility of traceability data. Keshta et al.[24] construct an agent-heavy encryption algorithm based on SM2 and blockchain, blockchain data sharing can provide a secure way for organizations to store and share data. Song et al.[25] designed a blockchain-based data traceability sharing mechanism to provide evidence for data authenticity and used proxy re-encryption to ensure the security and privacy of data sharing. Agyekum et al.[26] proposed a proxy re-encryption approach to protect data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while the proxy re-encryption construct will grant legitimate users access to the data.

In this study, BBPR-AC is proposed to address the problem of sharing private information in the field of agricultural biological risk information security. The approach deeply integrates blockchain and proxy re-encryption technologies and automates the determination of data-sharing permissions by improving the privacy protection process and simplifying the access control process, thus ensuring the secure, timely, and rapid sharing of private information on biological risk factors of agricultural products. This approach helps to prevent problems such as loss of trade secrets, misleading regulation, and social panic.

Blockchain-based proxy re-encryption access control method

Data analysis of agricultural biological risk factors

The protection of biological risk factor data of agricultural products is crucial, involving business secrets and production details. While ensuring open data traceability along the entire chain of agricultural supply chain, how to safely and reliably share relevant biological risk factor information, avoid information leakage, block agricultural products with high-risk factors, and reduce food safety incidents is the main research direction of this study. This study, concerning the Circular of the National Health and Wellness Commission of the People's Republic of China on the Issuance of Foodborne Disease Surveillance and Reporting Standards (for Trial Implementation) and the General Standards of Biological Safety for Virus Microbiology Laboratories of the People's Republic of China for Health Industry Standards, the biological risk factors of agricultural products were classified into four categories based on the infectiousness of pathogenic microorganisms, and the degree of harm that they can cause to an individual or a group of people after infection, as shown in Table 1.

When tracing the biological risk factors of agricultural products, it is important to record the public traceability information for each link of the agricultural products. This helps in blocking the traceability of biological risk factors. These factors are categorized into biological risk traceability information, secondary biological risk privacy information, and primary biological risk privacy information based on their privacy level and traceability role. The detection information of biological risk factors in Categories I and II of agricultural

Level	Definition
Category I biological risk factors	It is capable of causing very serious diseases in humans or animals, highly infectious microorganisms, as well as microorganisms that have not yet been discovered or have been declared eradicated in our country
Category II biological risk factors	It is a microorganism capable of causing serious disease in humans or animals and is relatively easy to transmit directly or indirectly from human to human, animal to human, or animal to animal
Category III biological risk factors	A microorganism that is capable of causing disease in humans or animals, but generally poses no serious harm to humans, animals, or the environment, has a limited risk of spreading, and for which effective treatment and prophylaxis are available
Category IV biological risk factors	Microorganisms that do not normally cause disease in humans or animals

Table 1. Levels of biological risk factors for agricultural products. Note: Categories I and II biological risk factors are referred to as highly pathogenic risk factors.

products is considered the first level of privacy information, while the privacy information of biological risk factors in Categories III and IV is considered the second level of privacy information. All public and private biological risk data should be accessible to credible regulators. The key data for biological risk factor detection of agricultural products are shown in Table 2. Regulators can access public data through the blockchain network, while first and second-level private data are shared with regulators by data owners through encrypted data sharing. Consumers can view publicly traceable data on the biological risks they are concerned about, but they are unable to access first-level and second-level biological risk privacy information. First-level and second-level privacy data mainly consist of the results of biological risk factor testing at various stages of the agricultural supply chain. These data have high confidentiality requirements are shared through privacy data sharing with authorized data visitor and are not visible to unauthorized users. The information model for traceability of agricultural biological risk factors is illustrated in Fig. 3.

Design of BBPR-AC method for traceability of biological risk factors in agricultural products

The production of agricultural products involves multiple stages, and the confidentiality of test results for biological risk factors is critical. The secure transmission of these test results helps to strengthen the control of food safety by regulatory agencies and to improve the quality of agricultural products and the efficiency of production. To protect the data privacy and security of agricultural biological risk factors, we propose the BBPR-AC framework. The approach incorporates access control, blockchain, and proxy re-encryption technologies to simplify the data-sharing process. Automated access control through smart contracts guarantees transparency and traceability. The characteristics of blockchain ensure the security and non-comparability of decision-making. BBPR-AC effectively addresses the challenges in traditional proxy re-encryption, improves the security and trustworthiness of sensitive data in the agricultural supply chain, and solves the problem that the data of biological risk factors in the agricultural supply chain can't be traced and efficiently regulated securely and flexibly.

Proxy re-encryption design of BBPR-AC

Proxy Re-encryption (PRE) is a cryptographic encryption technique that performs a secure transformation of a ciphertext. Traditional PRE is a public key encryption scheme that allows the data owner to "delegate" decryption rights to another data accessor. The data owner may delegate to a semi-trusted agent the task of transforming a ciphertext encrypted by itself into a ciphertext equivalent to the one encrypted by the data visitor (which can be decrypted by the data visitor's private key). The participants in the proxy re-encryption process are mainly categorized into three parties: the data owner, the data accessor, and the proxy. The main steps are as follows:

Agricultural supply chain link	Public information on biological risks	Second-level biological risk Privacy Information	First-level biological risk privacy information
Farm	Source of agricultural seeds, sowing date, plot information, production batch number, farming enterprises, etc	Information on the detection of biological risk factors for farming categories III and IV	Information on the detection of biological risk factors for farming categories I and II
Cultivation	Breed source, breeding start date, feed formulation, production batch number, breeding enterprise, etc	Information on the detection of risk factors for aquaculture category III and IV organisms	Information on the detection of biological risk factors for aquaculture category I and II organisms
Harvest	Harvest date, place of origin, picker information, production lot number, harvesting company, etc	Harvesting information on the detection of category III and IV biological risk factors	Harvesting information on the detection of category I and II biological risk factors
Processed product	Processing date, processing plant name, processing technology, production batch number, processing enterprise, etc	Information on the testing of biological risk factors for processed products categories III and IV	Information on the testing of biological risk factors for processed products categories I and II
Warehouse	Storage date, storage temperature, storage location, production batch number, storage enterprise, etc	Information on the testing of biological risk factors for storage categories III and IV	Warehousing information on the detection of category I and II biological risk factors
Transportation	Date of commencement and termination of transport, means of transport, route of transport, production batch number, transport enterprise, etc	Information on the detection of biological risk factors for transport categories III and IV	Transport information on the detection of category I and II biological risk factors
Distributor	Date of product purchase, source, name of distributor, production batch number, etc	Dealer Category 3 and 4 biological risk factor testing information	Dealer Class I and Class II biological risk factor testing information
Retailers	Product shelf date, place of sale, promotions, production batch number, retailer, etc	Information on retailer testing for category 3 and 4 biological risk factors	Information on retailer testing for Category 1 and 2 biological risk factors

Table 2. Key data of biological risk factor detection of agricultural products.

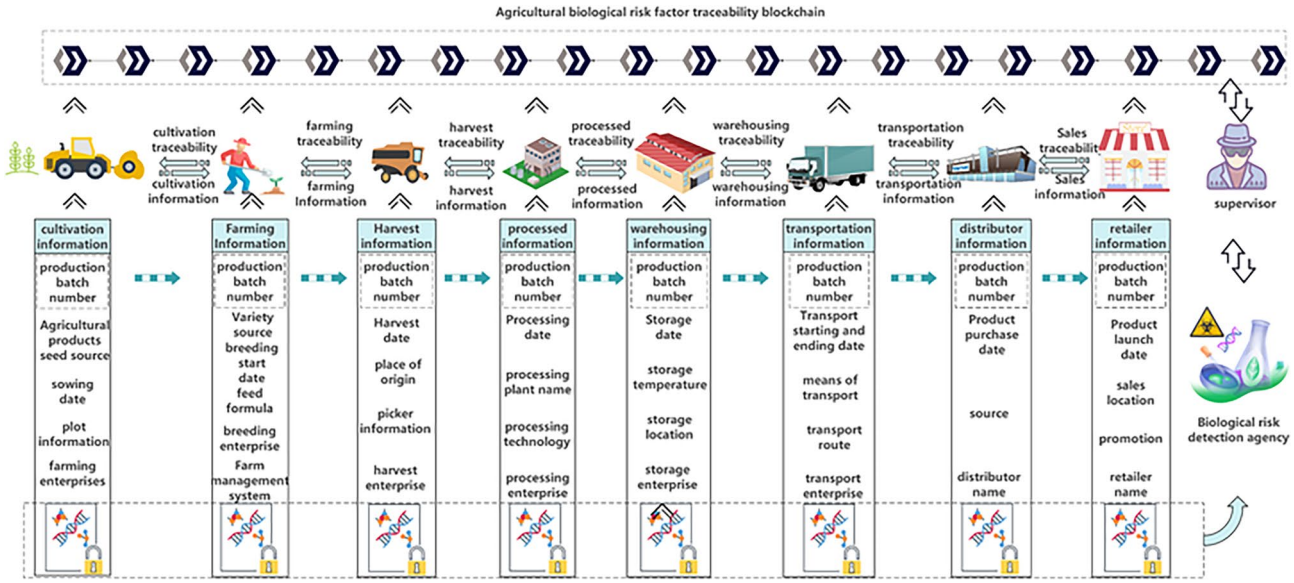


Fig. 3. Information model for traceability of biological risk factors of agricultural products.

1. Key generation: The data owner generates a pair of public and private keys for himself to ensure the security and control of the data.
2. Encrypt data: The owner encrypts the data using the public key to protect the confidentiality of the data in the cloud storage.
3. Construct re-encryption key: When it is necessary to share data with other users, the data owner generates a re-encryption key based on his/her private key and the recipient's public key.
4. Proxy re-encryption: The proxy server uses the re-encryption key to convert the data from one user's public key to another user's public key for secure data sharing. The proxy re-encryption process is shown in Fig. 4.

The traditional PRE uses an asymmetric encryption system that is inefficient and inappropriate for data sharing of larger files, so the PRE process needs to be optimized. In this study, symmetric encryption is used to protect the biological risk factor information, PRE is used to protect the symmetric key for symmetric encryption, and the encryption module is designed to be improved based on threshold proxy re-encryption. The proxy re-encryption used is based on the secp256k1 elliptic curve public key cryptosystem with the curve equation:

$$y^2 = x^3 + 7 \tag{1}$$

where x and y denote coordinate points in the two-dimensional plane, the x-axis denotes the horizontal coordinates and the y-axis denotes the vertical coordinates. For any point P(x,y), it is on this elliptic curve if and

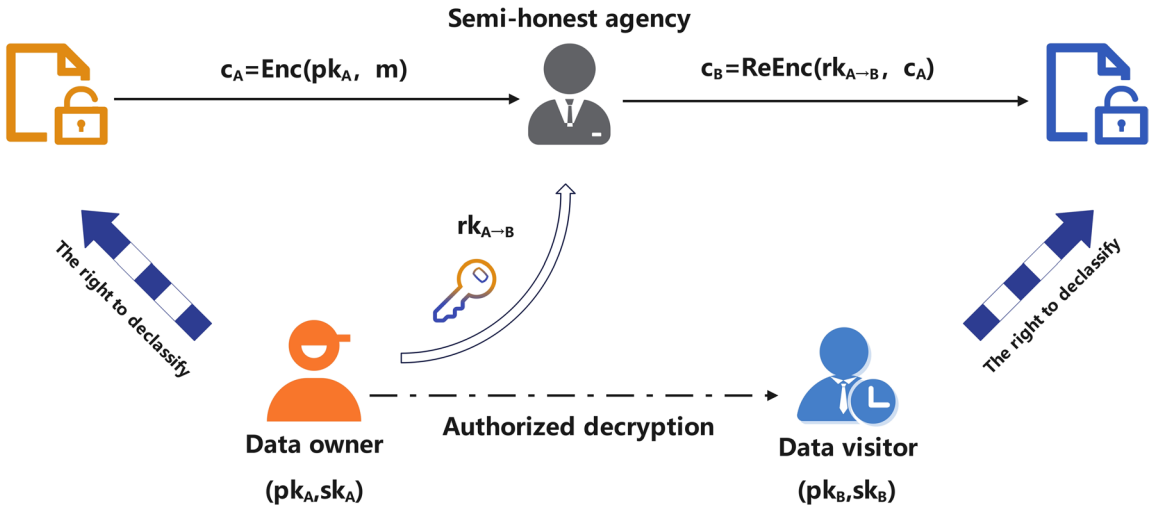


Fig. 4. Proxy re-encryption simple process.

only if it satisfies. The flow of encryption and decryption algorithm for symmetric encryption agent re-encryption is shown in Fig. 5.

1. Setting public parameters

- Setup(sec): this algorithm determines a cyclic group of prime order q according to the security parameter sec G. Let g, U$\in G$.Let $H_2 : G^2 \rightarrow Z_q$, $H_3 : G^3 \rightarrow Z_q$ and $H_4 : G^3 \times Z_q \rightarrow Z_q$.Let $KDF : G \rightarrow \{0,1\}^{\ell}$ be a key derivation function as a model of a stochastic prediction machine, and ℓ be set according to the security parameter sec. H is the hash function of the random field, Z_q denotes a cyclic group G of prime order q, which is used to denote the range of values of the elements in the group G. H_2 is commonly utilized for deriving values from two group elements to ensure even distribution of the output over Z_q. H_3 is employed in re-encryption key generation to derive the value d from a combination of three group elements, which is crucial for non-interactive Diffie-Hellman key exchange. H_4 is used in generating the re-encryption key fragment to calculate z_1, ensuring even distribution and dependency on multiple inputs, thereby enhancing the security of the scheme. Global public parameters are represented by tuples:

$$params = \left(G, g, U, H_2, H_3, H_4, KDF\right) \tag{2}$$

2. 2. Generate key algorithm

- KenGen(): The key generation algorithm KeyGen uniformly and randomly selects $a \in Z_q$, and outputs a pair of public keys and keys of agricultural biological risk factor testing organizations $(pk_A, sk_A) = \left(\mathrm{g}^{\mathrm{a}}, a\right)$.
- ReKeyGen $\left(sk_A,\ pk_B,\ N,\ t\right)$: Inputting the detection agency key $sk_A = a$ as well as the authorized public key $pk_B = \mathrm{g}^{\mathrm{b}}$, the number of segments N, and the threshold value t, ReKeyGen() generates N segments of the re-encryption key between the biological risk detection agency and the visitor, and each segment is named *KFrag*, the specific process is as follows:

(1) Sample random $\mathrm{x_A} \in Z_{\mathrm{q}}$ and compute $X_{\mathrm{A}} \in \mathrm{g}^{\mathrm{x}A}$.
(2) Compute $d = H_3\left(X_A,\ pk_B,\ \left(pk_B\right)^{xA}\right)$. d is the result of a non-interactive.
Diffie-Hellman key exchange between B's keypair and the ephemeral key pair $(x_A,\ X_A)$.
(3) Sample random $t-1$ elements $f_i \in Z_{\mathrm{q}}$, with $1 \le i \le t-1$, and compute $f_0 = a \cdot d^{-1} mod q$.
(4) Construct a polynomial $f(x) \in Z_q[x]$ of degree $t-1$, such that $f(x) = f_0 + f_{1x} + f_{2x_2} + \cdots + f_{t-1x_{t-1}}$.
(5) Compute $D = H_6\left(pk_A,\ pk_B,\ pk_B^{\mathrm{a}}\right)$.
(6) Initialize set $KF = \emptyset$ and repeat N times:

(a) Sample random $y, id \in Z_{\mathrm{q}}$.
(b) Compute $s_x = H_5(id,\ D)$ and $Y = g^y$.
(c) Compute $rk = f(s_x)$.
(d) Compute $U_1 = U^{rk}$.
(e) Compute $z_1 = H_4\left(Y,\ id,\ pk_A,\ pk_B,\ U_1,\ X_A\right)$, and $z_2 = y - a \cdot z_1$.
(f) Define a re-encryption key fragment *kFrag* as the tuple $(id,\ rk,\ X_A,\ U_1,\ z_1,\ z_2)$.

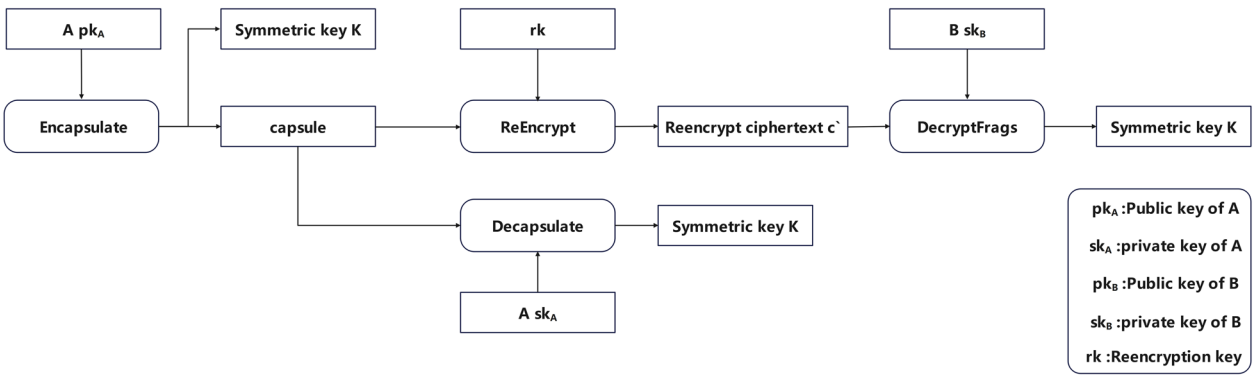


Fig. 5. Symmetric encryption proxy re-encryption algorithm flow.

(7) Finally, output the set of re-encryption key fragments KF. The number of segments N of the re-encryption key in the agent re-encryption as well as the threshold value are set to 1 in this study.

3. Encapsulation and decapsulation algorithms

- Encapsulate (pk_A): On input the public key pk_A, the encapsulation algorithm Encapsulate first samples random r, $u \in Z_q$ and computes $E = g^r$ and $V = g^u$. Next, computes the value $s = u + r \cdot H_2(E, V)$. The derived key is computed as $K = KDF\left((pkA)^{r+u}\right)$. The tuple (E, V, s) is called *capsule* and allows to derive again (i.e., "decapsulate") the symmetric key K. Finally, the encapsulation algorithm outputs $(K, capsule)$.
- CheckCapsule $(capsule)$: On input a $capsule = (E, V, s)$, this algorithm examines the validity of the capsule by checking if the following equation holds:

$$g^s = V \cdot E^{H2(E,V)} \tag{3}$$

- Decapsulate $(skA, capsule)$: On input the secret key $sk_A = a$, and an original $capsule = (E, V, s)$, the decapsulation algorithm Decapsulate first checks the validity of the capsule with CheckCapsule and outputs $\perp$ if the check fails. Otherwise, it computes $K = KDF((E \cdot V)a)$. Finally, it outputs K.

4. Re-encryption algorithm

- ReEncapsulate $(kFrag, capsule)$: On input a re-encryption key fragment $kFrag = (id, rk, X_A, U_1, z_1, z_2)$, and a $capsule = (E, V, s)$, the re-encapsulation algorithm ReEncapsulate first checks the validity of the capsule with CheckCapsule and outputs $\perp$ if the check fails. Otherwise, it computes $E_1 = E_{rk}$ and $V_1 = V_{rk}$, and outputs the capsule fragment $cFrag = (E_1, V_1, id, X_A)$.

5. Decryption algorithm

- DecapsulateFrags $(sk_B, pk_A, \{cFrag_i\}_{i=1}^{t})$: On input the secret key $sk_B = b$, the original public key $pk_A = g^a$, and a set of t capsule fragments, being each of them $cFrag_i = (E_1, i, V_1, i, id_i, X_A)$, the fragments decapsulation algorithm DecapsulateFrag does the following:

(1) Compute $D = H_6(pk_A, pk_B, pk_A^b)$.
(2) Let $S = \{s_{x.i}\}_{i=1}^{t}$, for $s_{x,i} = H5(id_i, D)$. For all $s_{x,i} \in S$, compute:

$$\lambda_{i,s} = \prod_{j=1, j\neq i}^{t} \frac{s_{x,j}}{s_{x,j} - s_{x,i}} \tag{4}$$

(3) Compute the values:

$$E' = \prod_{i=1}^{t} (E_{1,i})^{\lambda_{i,s}} \tag{5}$$

$$V' = \prod_{i=1}^{t} (V_{1,i})^{\lambda_{i,s}} \tag{6}$$

(4) Compute $d = H_3(X_A, pk_B, X_A^b)$. Recall that d is the result of a non-interactive Diffie-Hellman key exchange between B's keypair and the ephemeral key pair (x_A, X_A). Note also that the value X_A is the same for all the *cFrags* that are produced by re-encryptions using a *kF rag* in the set of re-encryption key fragments KF.
(5) Finally, output the symmetric key $K = KDF\left((E' \cdot V')^d\right)$.

The assigned values for capsule fragments and re-encryption key fragments in this study are both set to 1. Upon acquiring the symmetric key, individuals accessing the biological risk factor data of agricultural products can utilize it to decrypt the encrypted ciphertext within the agricultural products traceability blockchain system.

Access control design of BBPR-AC

Traditional access control models, such as autonomous access control (DAC), mandatory access control (MAC), and role-based access control (RBAC), have limitations in providing secure and effective information protection mechanisms in large-scale and complex network environments[27]. ABAC (Attribute-Based Access Control) is an access control model that controls access rights by defining policies between user attributes and object attributes. Compared with traditional role-based access control, ABAC is more flexible and can achieve fine-grained access control to improve system security and management efficiency[28].

This study proposes the BBPR-AC method for encrypted data sharing of biological risk factors for agricultural products. The method securely delivers biological risk data by automating permission verification on the chain, allowing data owners to decide whether to enable proxy re-encryption based on set access rights. This mechanism is designed to prevent social panic, declining corporate trust, malicious extortion, and food safety incidents caused by data leakage. At the same time, it simplifies the authorization process and improves the automation and security of the system. Five main subjects are involved in the access control module of this research design: subject, object, action, environment, and strategy. For this research discourse, the following definitions are given:

Definition 1. The attribute identification item is the most basic unit used to represent an attribute in an access control policy and adopts the format of *{xAttrName = attrValue}*, where *xAttrName* denotes the attribute name and *attrValue* denotes the attribute value. To facilitate the representation of different types of attributes, x is introduced to denote the attribute type, where *{s, r, a, e}* represents the access to the subject attribute of the visitor of the biological risk factor, the object attribute of the biological risk factor, the action attribute, and the environment attribute, respectively.

Definition 2. An attribute identity tuple is a collection of attribute identity items of the same type, denoted by *xAttrTuple, x* ∈ *{s, r, a, e}, i.e.: xAttrTuple:{(xAttrName1 = attrValue1)*∧ *(xAttrName2 = attrValue2)*∧…∧*(xAttrNamei = attrValuei)}*.

Definition 3. Access Request (AR) is composed of a set of tuples of visitor attributes, biological risk factor object attributes, action attributes, and environment attribute identifiers, denoted by *AR:{sAttrTuple*∧*rAttrTuple*∧*aAttr Tuple*∧*eAttrTuple}*. The meaning of AR is that a request for action *aAttrTuple* for biological risk factor *rAttrTuple* is made in the case of requesting visitors with the attribute *sAttrTuple*, in the case of an environment attribute is *eAttrTuple*, the request for action *aAttrTuple* on the biological risk factor *rAttrTuple*.

Definition 4. An access control rule is a set of access control policies for private information about different biological risk factors that reflects the authorization behavior of the information owner. The set of attribute identification tuples required to access a protected biological risk factor is specified and is denoted by *Rule:res ult(R,action,ruleID)* ← *Θ{xAttrTupleSet}signature_owner,x* ∈ *{s,r,a,e}*. where *Θ{xAttrTupleSet}* denotes a logical expression consisting of the identity tuples in the set of attribute identity tuples *xAttrTupleSet* through logical relations such as merge and disjunction, and *ruleID* denotes the unique identity of the rule. A visitor can be allowed to perform an action operation on a biological risk factor object R with *result* ∈ *{Permit, Deny}* when the attribute identification tuple owned by the visitor makes *Θ{xAttrTupleSet}* true. Biological risk factor access authorization rules need to be saved in a blockchain smart contract after negotiation and authorization by the testing organization, the relevant companies, and the regulator to ensure the authenticity and non-tampering of the policy[29].

In this study, a blockchain-based data access control framework for biological risk factors is constructed to optimize information sharing and privacy protection in the agricultural supply chain. A repository of business subject attributes, including identity, role, organizational, and temporal attributes, has been created by analyzing the various segments, collaboration patterns, and characteristics of the supply chain to ensure the authenticity and appropriateness of data access. At the same time, the biological risk factor data is divided into segments of the supply chain and given different levels of confidentiality and unique identifiers. The environment setting takes into account the impact of time variation on access privileges and allow access to specific data within a specific period. Operations include querying and writing for effective management of data. Policy formulation designs a set of access control policies based on subject attributes, object attributes, environments, and operations, such as the query operation of the regulatory authority on public data within a specific period. The framework automates the processing of access requests through the BBPR-AC mechanism, improving the efficiency and security of access control. This study combines the above analyses and traceability scenarios of agricultural biological risk factors to make the following attribute classifications, as shown in Table 3.

The access control module of the BBPR-AC framework is mainly divided into the preparation phase and the execution phase. The preparation phase is the process of publishing, updating, revoking attributes, establishing relationships between attributes, formulating access control policies, and responding to attribute queries; the execution phase is the process of judgment, decision-making, and execution of the response to requests by invoking the smart contracts of each part.

1. Preparation phase: Members of the various segments of the agricultural supply chain and the regulatory authorities work together to form an enterprise certification team, EC, through which a digital identity certificate is established using PKI (the PKI part does not belong to the focus of the discussion of this program, and will not be repeated here). Enterprises in the supply chain jointly publish attribute and

Attribute category	Property name	Attribute meaning
Biological Risk Traceability Enterprise Subject Attributes	ID	Unique identification of agricultural supply chain subjects
	UserID	Agricultural supply chain user identification (business, regulatory, consumer)
	Role	Role of the business entity in the agricultural supply chain (administrator or regular user)
	Org	Organizations belonging to business entities in the agricultural supply chain
	OrganizationType	Type of organization to which the business belongs (manufacturing, distribution, transport, regulation, consumption)
	Stage	Stage of business entity (production, processing, warehousing, transport, distribution, retail)
Biological Risk Factor Attributes	ID	Unique identification of the requested biological risk factor
	ProductID	Biological Risk Factor Product Labelling
	BatchID	Biological Risk Factor Product Lot Labelling
	Level	Confidentiality level of the requested biological risk factor object
	FullExternalTraceData	Biological risk factor retrospective public data
	Org	The organization to which the requested biological risk factor belongs
	Stage	Stage of the requested biological risk factor (production, processing, storage, transport, distribution, retail)
Operational Properties	Read	read operation
	Write	write operations
Environmental Properties	Geolocation	The source address when the request was initiated
	Destination Location	target address
	StartTime	Start time when the request was initiated
	EndTime	End time when the request is initiated

Table 3. Biological risk factor BBPR-AC access control attribute description.

attribute relationship information and issue attribute-based *xAttrTuple* for each enterprise and regulator, store the corresponding *xAttrTuple* to the AMP (Attribute management point), the AMP transmits the enterprise *xAttrTuple* and biological risk factor *xAttrTuple* to the PMP (Policy management point). Transfer to PMP(Policy management point), the biological risk factor information owner combines the information description of each enterprise, regulator, and environmental attribute in PMP to formulate a Rule, and store the signed $Rule{:}result(R,action,ruleID) \leftarrow \Theta\{xAttrTupleSet\}_{signature\_owner}$ is stored to the PMP.

2. Execution phase: the biological risk factor information accessor brings up $AR{:}\{sAttrTuple \wedge rAttrTuple \wedge aAttrTuple \wedge eAttrTuple\}$, as shown in the steps in Figure 2.1. PEP (Policy execution point) receives a certain access request from a visitor to the privacy information of an agricultural product biological risk factor test report of a certain link, parses out the semantics of the corresponding enterprise, the biological risk factor object that it wants to access, the operation, etc. in the original request, and sends the *xAttrTuple* corresponding to each item in the original request to the AMP, which determines the authenticity and returns the result to PEP, as shown in steps 2.2 and 2.3 of Fig. 6. The PEP submits each *xAttrTuple* returned to the PDP (Policy decision point), which receives the parsed AR and makes a Rule request to the PMP, as shown in steps 2.4 and 2.5 of Fig. 6. PMP returns the corresponding Rule to PDP based on $AR{:}\ result(R,action,ruleID) \leftarrow \Theta\{xAttrTupleSet\}_{signature\_owner}$, PDP makes a policy decision based on the Rule, i.e., whether to allow the visitor to carry out the corresponding operation on the biological risk factor detection information. $result == Permit$ or *Deny*, as shown in steps 2.6 and 2.7 of Fig. 6. The PDP returns the policy result to the PEP, which decides whether or not to authorize the biological risk factor visitor to perform the corresponding operation based on the returned result, as shown in steps 2.8 and 2.9 of Fig. 6.

The BBPR-AC access control module workflow is shown in Fig. 6.

BBPR-AC mechanism framework and process

BBPR-AC is an access control system for traceability of biological risk factors of agricultural products, which is mainly divided into access control links and re-encryption links. Taking the biological risk factor testing organization as the data owner as an example, the overall process of BBPR-AC is described in detail.

After the biological risk factor visitor is authenticated based on PKI and obtains its subject attribute and biological risk factor object attribute through the collaboration of all parties in the agricultural supply chain, it initiates an access request $AR{:}\{sAttrTuple \wedge rAttrTuple \wedge aAttrTuple \wedge eAttrTuple\}$ to the agricultural product traceability blockchain system, as shown in Steps 1 and 4 in the left part of Fig. 7. A re-encrypted ciphertext is obtained when the biological risk factor visitor's attribute information meets the authorization settings of the access control mechanism. This ciphertext can be decrypted by the visitor's private key to obtain the final biological risk factor detection report. Visitors can obtain a validation hash through the Agricultural Biological Risk Traceability Blockchain, thereby verifying the correctness of the report content. As shown in the left step of Fig. 7. The access control module of the biological risk traceability blockchain obtains the *sAttrTuple*, *rAttrTuple*, *aAttrTuple* and *eAttrTuple* attributes in the access request by parsing the AR and arrives at a response of whether to authorize or not based on the built-in set of attributes of the AMP, PMP, PDP, and PEP smart contracts, as well

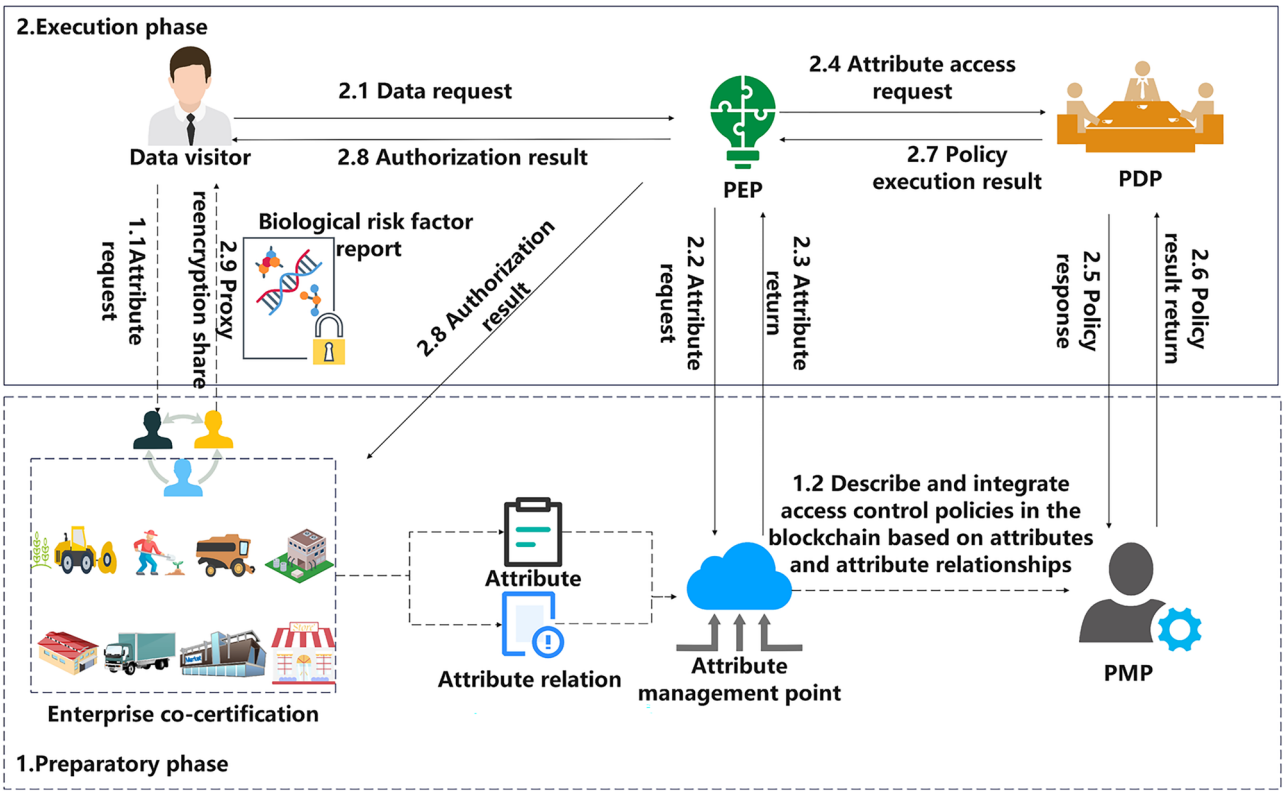


Fig. 6. BBPR-AC Access control process.

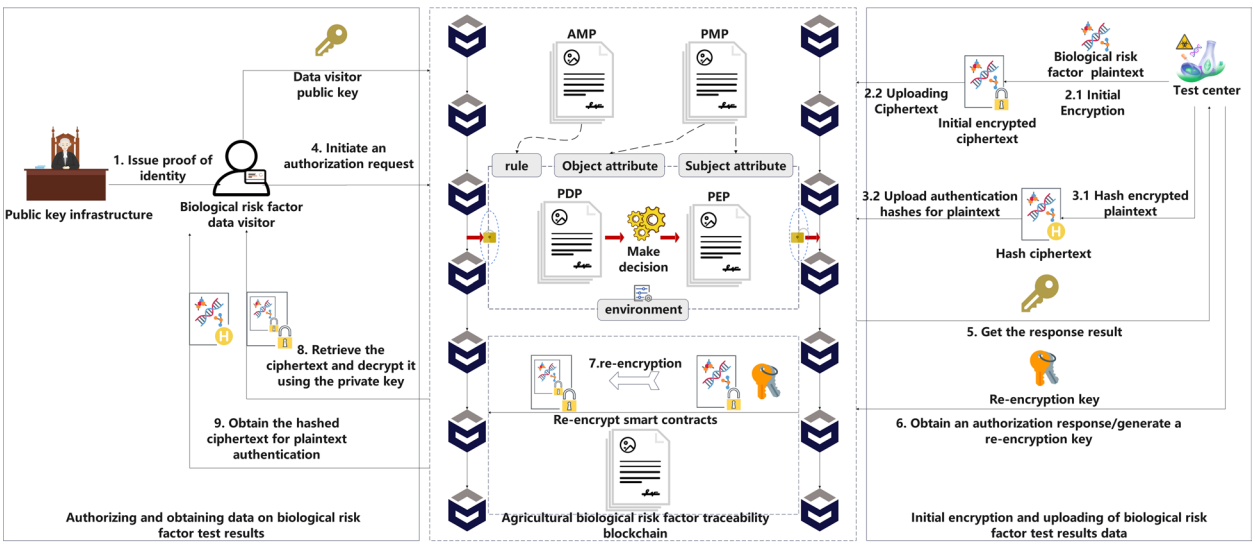


Fig. 7. BBPR-AC data encryption and sharing process.

as the policy selection. The Biological Risk Factor Testing Center decides whether to share biological risk factor data appropriately based on supply chain collaboration needs. The biological risk factor testing center carries out the initial encryption of the biological risk factor in proxy re-encryption based on its own public key, and uploads the ciphertext after the initial encryption to the agricultural product biological risk traceability blockchain, as shown in Steps 2.1 and 2.2 in the right part of Fig. 7. The detection center uploads the authentication hash after encrypting the plaintext hash of the biological risk factor to the blockchain system, as in steps 3.1 and 3.2 in the right part of Fig. 7. After obtaining the request for authorization response, the biological risk factor testing center generates the proxy re-encryption key according to the public key of the visitor, as in steps 5 and 6 in the right part of Fig. 7. The biological risk factor testing center uploads the generated proxy re-encryption key of the visitor to the agricultural product biological risk factor traceability blockchain system, generates the biological risk factor proxy re-encryption cipher text by invoking the proxy re-encryption smart contract, and saves it to

the agricultural product traceability blockchain, as shown in steps 7 and 8 in Fig. 7. The biological risk factor data visitor obtains the biological risk factor proxy re-encrypted ciphertext by querying the biological risk factor traceability blockchain data. Finally, the visitor successfully decrypts the re-encrypted ciphertext using its private key to obtain the biological risk factor plaintext report, and the visitor obtains a verification hash through the blockchain system to verify that the decrypted plaintext has not been tampered with, as shown in the left part of Fig. 7, steps 9 and 10.

To visually illustrate the process of the methodology of this study, the BBPR-AC cryptographic sharing timing process is divided into the initial encryption and information uploading phase of the biological risk factor, the authentication and authorization phase of the biological risk factor, the re-encrypted transmission of the biological risk factor, and the plaintext validation phase of the biological risk factor, and the flow is shown in Fig. 8.

Experimental test and results

Design of experiments

In this study, we designed a blockchain network for agricultural product traceability based on Hyperledger Fabric. The test environment uses Hyperledger Fabric 2.4 and Hyperledger Explorer 1.1.8, built on Ubuntu 16.04 LTS virtual machine system, the experimental architecture is shown in Fig. 9.

The experiments use gRPC to send transactions directly through Tape and use the concatenation and channel cache for parallel processing, which improves processing efficiency. The BBPR-AC re-encryption link is based on the Nucypher platform to achieve the simulation. The nodes in the blockchain use CouchDB to store the uplinked data. The specific test environment configuration is shown in Table 4.

Smart contract design

This study is based on the Hyperledger Fabric platform, combined with the actual situation of the agricultural supply chain and other relevant smart contract rules. Part of the smart contract business logic design is shown in Table 5.

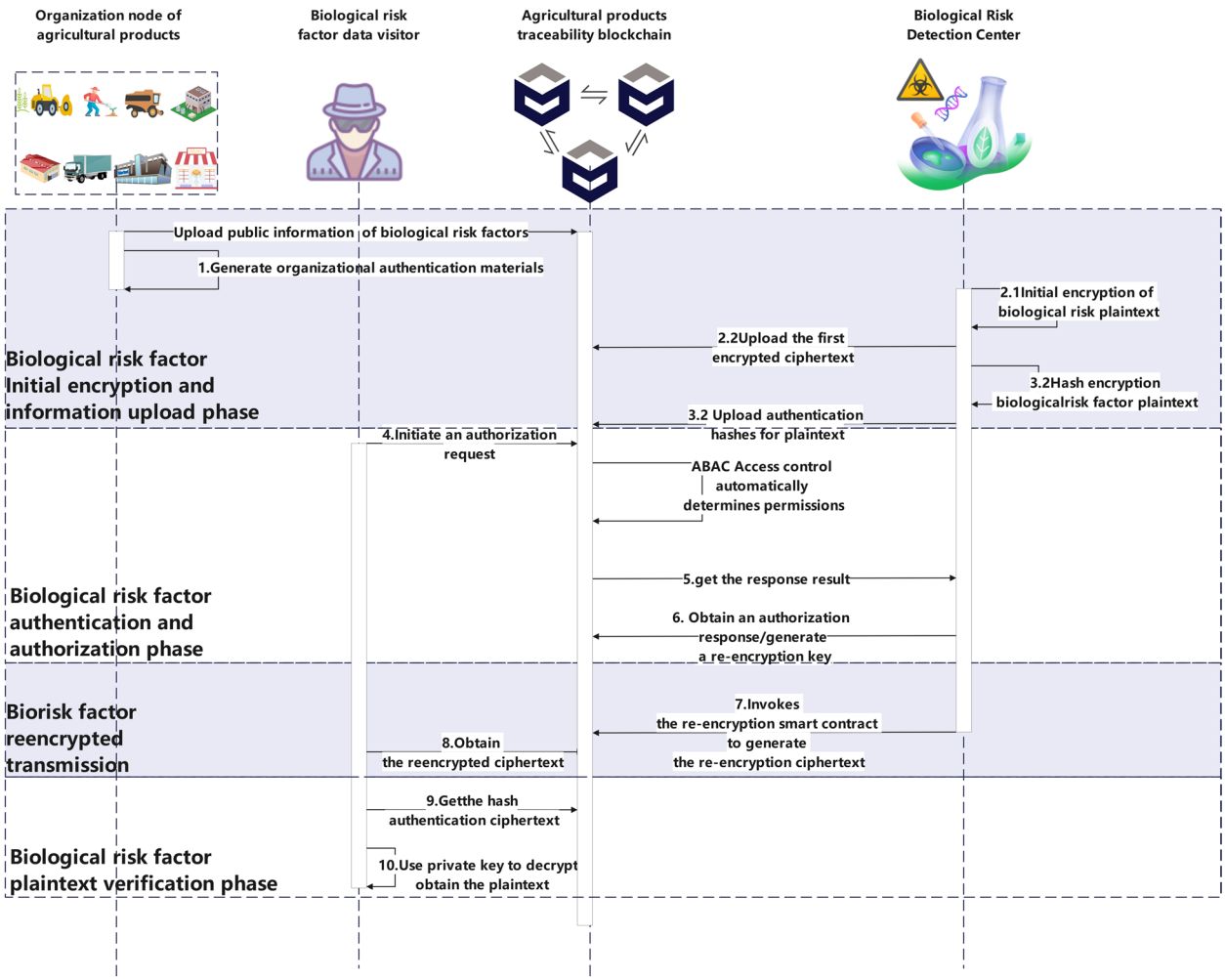


Fig. 8. BBPR-AC encryption sharing sequence process.

The functions of information traceability and BBPR-AC access control in each production and sales link of agricultural products are realized by smart contracts. Taking the policy determination in BBPR-AC access control as an example, the specific contract is as follows

```
Input: AR:{sAttrTuple∧rAttrTuple∧aAttrTuple∧eAttrTuple}

Output: True/False

function RecordcheckAccessPermission()

if len(args) then

    return shim.Error
    end if

    recordTotal1 ← getRecordByID(subjectID, stub)

    pb1, _ ← json.Marshal(recordTotal1)

    fmt.Printf("Query result: %s\n", pb1)

    var subject Subject

    err ← json.Unmarshal(pb1, &subject)

    if err != nil then

        return shim.Error("Error unmarshaling subject data: " + err.Error())

    end if

    recordTotal2 ← getRecordByID(objectID, stub)

    pb2, _ ← json.Marshal(recordTotal2)

    fmt.Printf("Query result: %s\n", pb2)

    var object Object

    err ← json.Unmarshal(pb2, &object)

    if err != nil then

        return shim.Error("Error unmarshaling subject data: " + err.Error())

    end if
```

```
recordTotal ← getRecordByName(subjectID, stub)

pb, _ ← json.Marshal(recordTotal)

fmt.Printf("Query Policy result: %s\n", pb)

if pb == nil then
    return shim.Error("Policy not found for the given subject and object IDs")
end if

var policy Policy

err ← json.Unmarshal(pb, &policy)

if err != nil then
    return shim.Error("Failed to unmarshal policy data: " + err.Error())

if policy.Object.ID == objectID && policy.Subject.ID == subjectID && policy.Action == action then
    return shim.Success([]byte("Access granted. Allowed to perform the action on the object."))
end if

return shim.Error("Access denied. Not allowed to act on the object.")

end function
```

Functional testing of the agricultural biological risk factor BBPR-AC

To test the effectiveness and various aspects of the efficiency of the BBPR-AC biological risk factor access control method proposed in this study, the experiment was designed for agricultural products' biological risk factor testing reports. The test uses the simulated report as the traceability privacy data of the biological risk factor, the biological risk factor testing organization as the data owner, and the regulatory body as the data accessor to test the BBPR-AC method. The biological risk factor report is in the form of a picture, as shown in Fig. 10a. Converted to Base64 strings, the test report of Xinjiang French small prunes was used as the data test object, and the sample test report was converted to Base64 strings, as shown in Fig. 10b.

Uploading of agricultural biological risk factor BBPR-AC preliminary encryption material

The inspection agency will pass the inspection report through the encryption link in BBPR-AC, the Base64 string of the biological risk factor inspection report will be encrypted for the first time, and the plaintext of the biological risk factor will be encrypted with a hash, as shown in Fig. 11a, and upload the above materials into the agricultural products' biological risk factor traceability blockchain, and the uploaded information is saved in the transaction id as transaction id as 47f1081efde8383b51df92c1d374d750658655b8762586e8a79af029e3eb4013 block, with a call chain code of victory, and the result is shown in Fig. 11b of the agricultural biological risk factor traceability blockchain browser.

Authorisation judgment for the agricultural biological risk factor BBPR-AC

The regulator invokes the BBPR-AC access control smart contract through the agricultural biological risk factor traceability blockchain and makes an access request to the biological risk factor test report of Xinjiang French small prunes. The BBPR-AC simulates the organizational aspects of the agricultural biological risk factor traceability blockchain, and cooperates to complete the formulation of the access subject, the biological risk factor object, the access environment, and the simulation strategy, and deploys it on the blockchain. The attribute

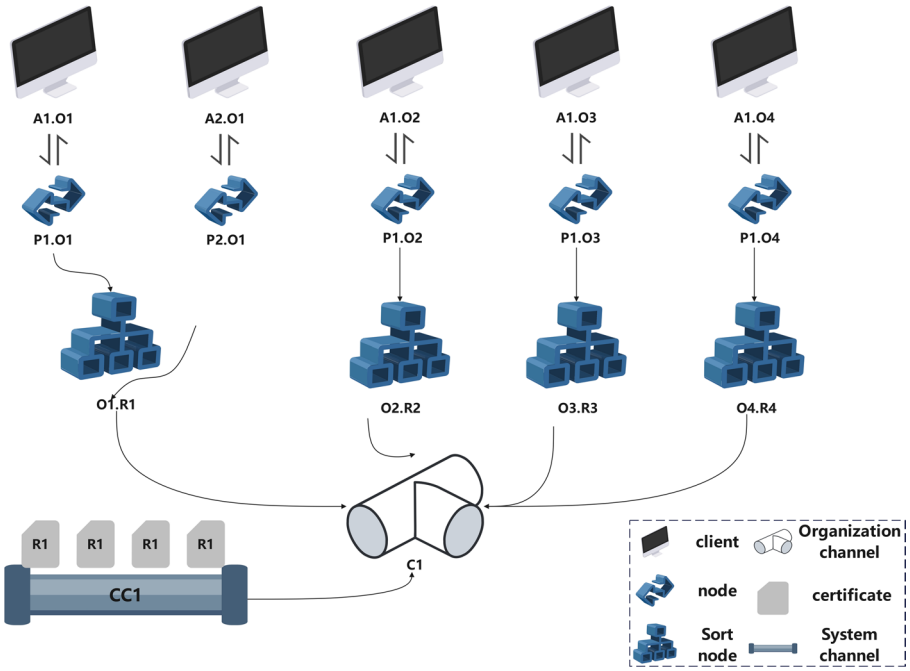


Fig. 9. Blockchain network configuration.

Blockchain configuration	Value	Description
Chains	1	Agricultural supply chain organizations, consumer organizations, regulators, and biological risk factor testing centers maintain a blockchain together
Number of organizations	4	Agricultural supply chain organizations, consumer organizations, regulator organizations, biological risk factor testing organizations
Number of nodes	5	2 organizational nodes for agricultural products, 1 organizational node for consumers, 1 organizational node for regulatory agencies, 1 organizational node for biological risk factor testing agencies
Comprehensive database	CouchDB	The entire blockchain uses a CouchDB state database to store the uplinked data
Consensus mechanisms	Raft	The Raft consensus mechanism is used so that all nodes in the blockchain work together to maintain the consistency of the ledger
Chunk time	1 s	Time to post transactions and package them to generate blocks
Maximum number of transactions in a block	10	Maximum number of transactions contained in each block
Maximum block capacity	10 MB	Maximum capacity of data stored in each block
Maximum storage space per transaction	512 KB	Maximum storage size of 512 KB per transaction

Table 4. Test environment configuration.

semantics and attribute value assignments are derived from AA, the agricultural product regulatory authority, to ensure the safety and reliability of the data. As shown in Table 6, the data on the left side indicates the attribute values of the relevant attributes, and the right side indicates the attribute relationships between the relevant attributes.

Based on the above attribute values and attribute relationships, the regulator calls the access control smart contract to add policy() method to upload and query the simulation policy $Rule{:}result(R,action{:}read,ruleID{:}1) \leftarrow \Theta\{1AttrTupleSet\}_{signature\_owner}\{1AttrTupleSet\}=\{sAttrTuple\{(sID=1)\wedge(sName=Farming\ organization)\wedge(sRole=admin)\}\wedge rAttrTuple\{(rID=10)\}\wedge aAttrTuple\{(allowAction=read)\}\wedge eAttrTuple\{(time=2024\text{–}03\text{-}04\wedge location=location1)\}\}$ as shown in Fig. 12a, b. Regulator initiates $AR{:}\{sAttrTuple\{(sID=1)\wedge(sName=Farming\ organization\ )\wedge(sRole=admin)\}\wedge rAttrTuple\{(rID=10)\}\wedge aAttrTuple\{(allowAction=read)\}\wedge eAttrTuple\{(time=2024\text{-}03\text{-}04\wedge location=location1)\}$, The regulator calls the BBPR-AC access control smart contract checkAccessPermission() method and returns the authorization success response, as shown in Fig. 12c. The unauthorized subject calls the access control smart contract checkAccessPermission() method and returns an authorization failure response, as shown in Fig. 12d.

Agricultural biological risk factor BBPR-AC authorization decryption

After obtaining the authorized response to the request of the regulator, the biological risk factor testing agency generates the biological risk factor re-encryption key and re-encryption material through BBPR-AC re-encryption, and uploads them into the agricultural products' biological risk factor traceability blockchain, and

Contract function	Contractual method	Description	Input	Output
Upload Biological Risk Factor BBPR-AC Access Control Information	addSubjectAttribute()	Write the information on agricultural biological risk factor traceability subjects into the blockchain	Information on Traceability Subjects of Agricultural Biological Risk Factors	True/False
	addObjectAttribute()	Write biological risk factor object information for each link in the agricultural supply chain into the blockchain	Agricultural Biological Risk Factor Object Information	True/False
	addPolicy()	Write the information of the designed access strategy for biological risk factors into the blockchain	Subject information, biological risk factor object information, environment, correspondence action	True/False
	setFixedEnvironment()	Writing environmental information involved in access control to the blockchain	Strategic Environmental Information	True/False
	Upload ()	Public traceability information of agricultural biological risk factors written on the chain	Biorisk factor traceability data	True/False
Biological Risk Factor Data Query	getRecordByID()	Traceability information by batch number	Agricultural batch number	Public or private information about the traceability of the produce with the corresponding batch number
	getRecordByName()	Query policy information by name	Name of the strategy	Policy name, information on subjects allowed to access, resource information, authorization action
Strategic decision making	checkAccessPermission()	Input information such as subject ID, subject attributes, resource ID you want to access, and actions to determine whether the subject has the relevant permissions	Subject ID, Subject Organisation, Subject Role, Subject Affiliated Link, Resource ID, Action	Authorization information. Returns authorization success if the permissions are correct, or authorization failure if the permissions are incorrect

Table 5. Smart contract logic design.

the results are shown in Fig. 13a and c. After obtaining the re-encrypted material, the regulatory body decrypts the Base64 string of the biological risk factor inspection report of Xinjiang French small prunes through its private key, which is then converted into the inspection report image by Base64, and successfully obtains the inspection report of the biological risk factor of the agricultural product, and the results are shown in Fig. 13b and d.

BBPR-AC performance test

Comparative analysis of BBPR-AC encryption methods for agricultural biological risks

Xuan et al.[30] propose a ring signature-based confidential transaction scheme to hide the transaction amount and protect transaction privacy and identity privacy using a ring signature. Youliang et al.[31] propose blockchain data traceability algorithms based on attribute encryption, design policy update algorithms applicable to the blockchain, and achieve dynamic protection of transaction privacy. Feng et al.[32] combining hierarchical attribute encryption with linear secret sharing, a blockchain data privacy protection control scheme based on searchable attribute encryption is proposed to solve the privacy exposure problem in traditional blockchain transactions. Khan et al.[33] propose a distributed usage control model called DistU. This model can continuously monitor resources during operations and update properties accordingly to perform different operations. In the following, a comparative analysis of the functional characteristics of this research and the encryption methods in existing research proposals is carried out concerning whether or not ciphertext data access control is supported, whether or not it is resistant to conspiracy attacks, whether or not it is re-encrypted, and whether or not the data is traceable, as shown in Table 7.

Performance analysis of the agricultural biological risk BBPR-AC encryption approach

In this study, the time consumption of each phase of the simulation experiment including key generation, encryption algorithm, and other operations is tested and the performance efficiency of this study is evaluated based on the experimental results. This study implements BBPR-AC encryption phase simulation based on Python 3.7.4. In this study, the whole privacy data sharing is divided into 4 phases: initial encryption ciphertext, generation of re-encryption key, re-encryption, and decryption. The computational efficiency of the 4 phases is analyzed and compared at 64, 128, 256, 512, and 1024B data plaintext sizes, and the average of 30 runs of the algorithm is taken as the experimental results. As shown in Fig. 14a, the consumption time of each BBPR-AC encryption session is stable for different plaintext sizes, with the initial encryption of the plaintext stable at 1.6 ms, the generation of the re-encryption key at roughly 2.7 ms, the generation of the re-encrypted ciphertext at 2.5 ms, and the decryption of the ciphertext at around 3.0 ms. In the experimental test, the number of re-encryption keys and re-encryption ciphertext generated is fixed. Therefore, there are no possible linear changes that are affected by the size of the data. Symmetric key encryption of plaintext is used in this research scheme with low and stable computational overhead. It achieves the dynamic adjustment of the access rights to the privacy data of agricultural products' biological risk traceability and meets the security sharing needs of biological risk factor testing organizations and third-party data accessors.

At present, the main methods of privacy data encryption and sharing in the field of agricultural safety traceability are symmetric encryption, asymmetric encryption, and the combination of symmetric encryption and asymmetric encryption. This study and the Advanced encryption standard (Advanced encryption standard, AES) algorithm, asymmetric encryption RSA algorithm, AES + RSA algorithm encryption, and decryption links were tested and compared respectively, and the experimental results were taken as the average value of the algorithms running 30 times. This study is scheme 1, AES is scheme 2, RSA is scheme 3, and AES + RSA is scheme 3. The results are shown in Fig. 14b. The BBPR-AC encryption phase proposed in this study consists of the initial encryption ciphertext and the re-encryption part, and the decryption phase represents the decryption of the re-encrypted ciphertext. With the same size of the plaintext, this study is smaller than the combination of asymmetric encryption and asymmetric encryption in the encryption part, consuming about 3.29 ms; the decryption part is slightly equal to scheme 3 and scheme 4, slightly larger than scheme 2, consuming 3.1 ms. the overall computational overhead is small, which is advantageous, and it can satisfy the practical needs of privacy data security sharing in agricultural products biological risk traceability scenarios.

Meanwhile, this study tested the CPU usage and memory consumption of four schemes with 256B plaintext size. The 512B plaintext can represent the overall situation after converting the privacy data of biological risk factors of agricultural products into base64 data. The main hardware of this experiment is 13th Gen Intel(R) Core(TM) i5-13500H 2.60GHz,16GB memory, and Windows 11 operating system. This study is scheme 1, AES is scheme 2, RSA is scheme 3, and AES + RSA is scheme 3. As shown in Fig. 15a and b, the experimental results indicate that the proxy re-encryption scheme used in this study exhibits slightly higher CPU usage compared to AES, AES + RSA, RSA, while its memory consumption is lower than the other three schemes. Overall, the system resource consumption performance is good.

Performance analysis of BBPR-AC access control for agricultural biological risks

In this section, we use comparative analysis to compare this paper's scheme with the proposed data-sharing schemes, and analyze the platform of the comparative model, whether it supports fine-grained access control, privacy protection, whether it supports attribute updating, whether it supports data tampering, and whether it supports the key factors of smart contracts, as shown in Table 8. Comparing this study with the existing research results from the above seven aspects, it can be seen that this model has certain advantages.

In this study, we design a privacy-preserving access control mechanism for biological risk factors based on attribute access control and conduct performance tests on the determination time of different numbers of request policies and the response time of requests with different numbers of policies. As shown in Fig. 16a, when the requests gradually increase and the number of policies is fixed, the request-response determination time is linearly increasing. This is because as the number of requests increases, the length of requests that need to wait for the contract to process increases. As shown in Fig. 16b, traversing each policy in the policy set and performing the determination, the determination latency increases with the increasing number of access requests, this is because the traversal space increases with the increase in the number of access control policies, and the complexity of the policy determination is also increasing.

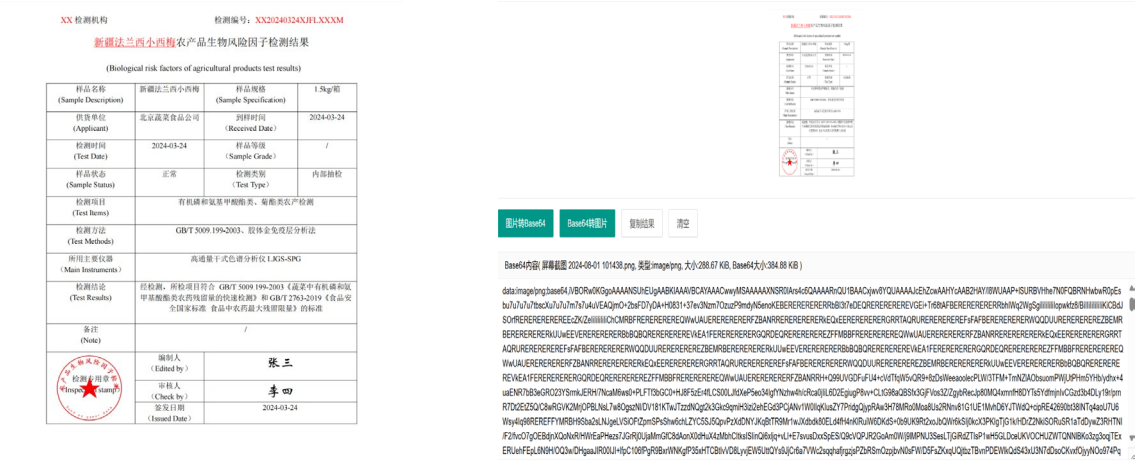
From the table, we know that the advantages of the study by Jianbiao et al., and this study are the same in the comparative analysis of the seven key factors mentioned above. To explore the relationship between the strategy evaluation time and the number of strategies, this study is compared with the scenarios outlined in the study by Jianbiao et al., by setting up the same number of requests with the number of attributes in the requests as 5, and repeat the 30 experiments to take the average, this study is scheme 1 and the study by Jianbiao et al. is scheme 2. The results are shown in Fig. 17. The method of this study uses indexing to speed up data retrieval and reduce access time. The strategy evaluation time in scheme 2 escalates rapidly with the increase in the number of strategies, and exhaustive traversal of all blocks is performed to retrieve strategies in the above scheme. The scheme proposed in this study shows stable performance with policy determination time around 2000–3000 ms as the number of policies increases and does not escalate rapidly with the increase in policy determination time.

Agricultural biological risk traceability blockchain performance analysis

The performance test of agricultural biological risk factor traceability blockchain uses the Tape test tool, and the results of the data uploading performance test are shown in Fig. 18a, the throughput of 30 rounds of uploading agricultural biological risk traceability data is 48.7 tx/s on average, which can satisfy the demand of real-time updating of agricultural biological risk traceability data of the upstream and downstream links of the supply chain of agricultural products. The data query performance test results are shown in Fig. 18b, the throughput of 30 rounds of data query of agricultural product traceability blockchain is 81.8 tx/s on average, which can meet the demand of relevant users for rapid query of agricultural product biological risk traceability information. From the above test results, it can be concluded that the data uploading and data querying time of the agricultural products biological risk factor traceability blockchain is stable, and it can meet the biological risk traceability needs of users in all links of the agricultural products supply chain.

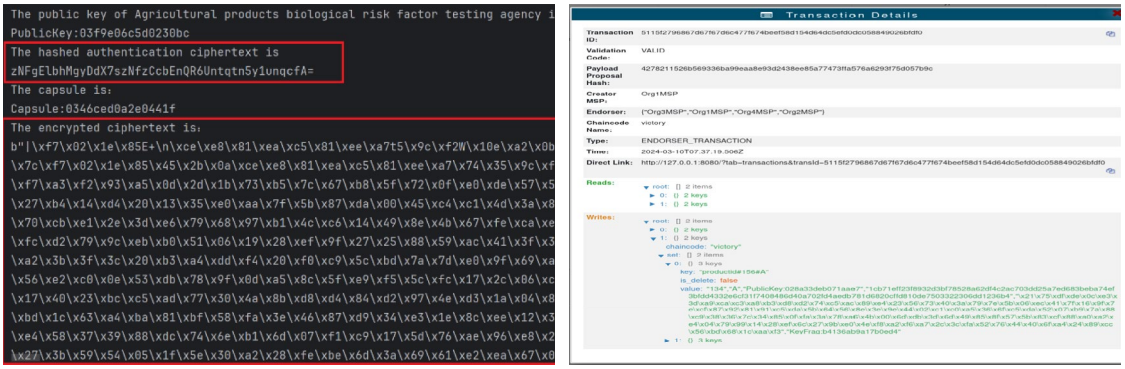
Conclusions

Ensuring the traceability and privacy of agricultural biological risks in the produce supply chain has become critical with the increase in biological risk factors. In this study, we propose a BBPR-AC-based method for agricultural biological risk privacy information protection, which achieves the traceability of agricultural biological risk and ensures the flexible authorization and secure sharing of privacy data by establishing an agricultural biological risk factor traceability blockchain. The BBPR-AC method avoids the complexity and centralization problems in the traditional authorization process by using proxy re-encryption and achieves decentralized encryption and automated authority determination through intelligent contract achieves decentralized encryption and automated



(a) (b)

Fig. 10. Little Prune biological risk factor simulation report. (**a**) Biological Risk Factor Test Report for Prunus macrocarpa (**b**) Conversion of reports to Base64 strings.



(a) (b)

Fig. 11. Initial BBPR-AC encryption phase. (**a**) BBPR-AC Initial encryption (**b**) Encrypted material uploaded to the blockchain.

permission determination, improving the efficiency, transparency, and security of the authorization process. Tests and analyses show that the method provides an effective solution for tracing biological risk information, privacy protection, and access control in the agricultural supply chain.

These efforts will provide solid technical support for new smart agriculture, promote the application of privacy-preserving technology and blockchain technology in agricultural supply chain systems, and provide useful references for research and practice in related fields.

The privacy protection method for biological risks traceability of agricultural products proposed in this study, BBPR-AC, offers advantages such as decentralized authorization and encryption. However, the method imposes certain hardware requirements on data owners and entails some performance overhead. Specifically, within BBPR-AC, data owners are required to carry out initial encryption of privacy data, generate re-encryption keys, and perform re-encryption on the blockchain chain. This necessitates that data owners possess hardware with a certain level of performance to complete these tasks within BBPR-AC; otherwise it will lead to increased time overhead and response time for the method.

As a result, the next focus of this research will be to reduce the workload for data owners by enhancing the integration of our research method with blockchain systems and optimizing processes to minimize performance overhead for data owners. Additionally, there will be a greater emphasis on deep integration of the blockchain network and re-encryption smart contracts for agricultural product biological risk factor traceability in order to provide more practical cases and validate the approach proposed in this study.

Attribute value	Attribute relationship
	sIdNameRelavant(1, *Farming organization*)
sID(1)	*sIdNameRelavant*(2, *Culture tissue*)
sID(2)	*sIdNameRelavant*(3, *Harvest tissue*)
sID(3)	*sIdNameRelavant*(4, *Regulatory agency*)
sID(4)	*rIdNameRelavant*(10, *Level 3 open data*)
sName(*Farming organization*)	*rIdNameRelavant*(20, *Level 2 privacy data*)
sName(*Culture tissue*)	*rIdNameRelavant*(30, *Level 1 privacy data*)
sName(*Harvest tissue*)	*roleAssignment*(1,*admin*)
sName(*Regulatory agency*)	*roleAssignment*(2,*user*)
sRole(*user*)	*roleAssignment*(3,*others*)
sRole(*admin*)	*roleAssignment*(4,*supervise*)
sRole(*supervise*)	*allowAction*(*Level 3 open data*, *update*)
sRole(*others*)	*allowAction*(*Level 3 open data*, *read*)
rID(10)	*allowAction*(*Level 3 open data*, *delete*)
rID(20)	*allowAction*(*Level 2 privacy data*, *update*)
rID(30)	*allowAction*(*Level 2 privacy data*, *read*)
rName(*Level 3 open data*)	*allowAction*(*Level 2 privacy data*, *delete*)
rName(*Level 2 privacy data*)	*allowAction*(*Level 1 privacy data*, *update*)
rName(*Level 1 privacy data*)	*allowAction*(*Level 1 privacy data*, *read*)

Table 6. Attributes and attribute relationships.

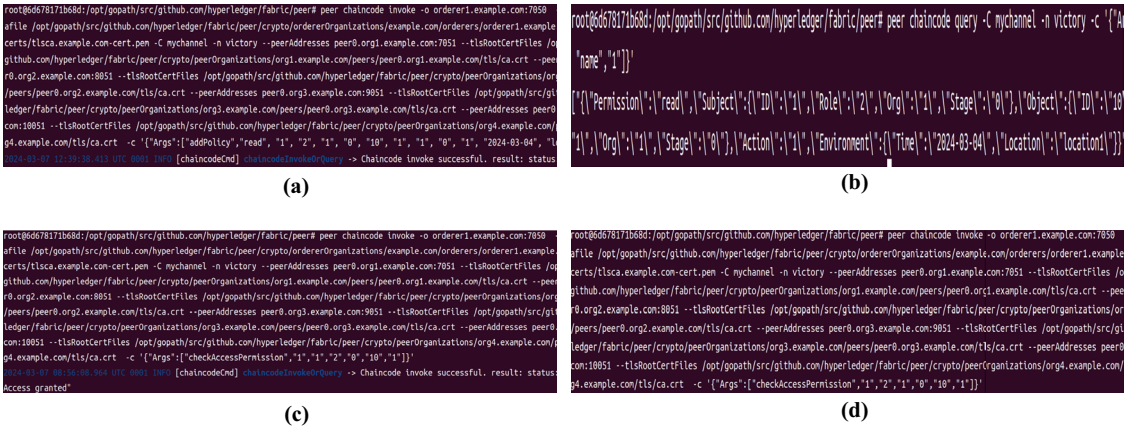


Fig. 12. BBPR-AC access authorization phase. (**a**) Upload Strategy (**b**) Query Strategy (**c**) Determination of successful authorisation (**d**) Determination of authorization failure.

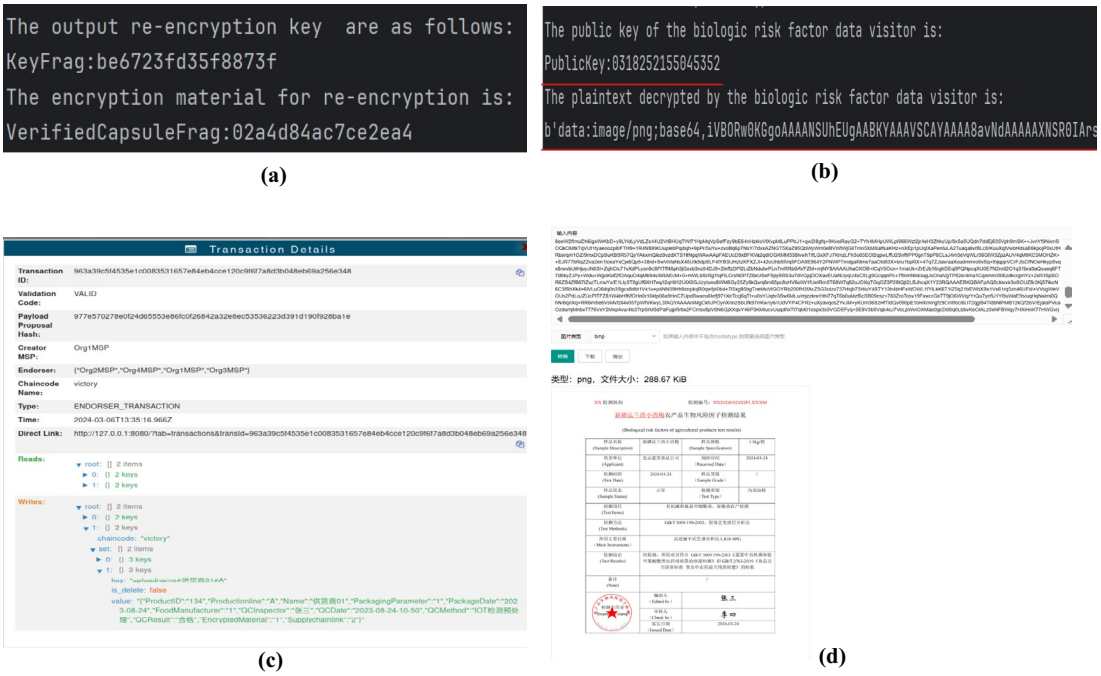


Fig. 13. Authorization decryption phase. (**a**) Testing organizations generate re-encrypted material (**b**) Regulators decrypt re-encrypted ciphertexts (**c**) Testing organisation upload re-encrypted material (**d**) Regulators convert Base64 characters to test reports.

Encryption method	Ciphertext access control	Resistance to conspiracy attacks	Re-encrypt	Traceable
Xuan et al.	×	√	×	√
Youliang et al.	√	×	×	√
Feng et al.	√	√	×	√
Khan et al.	√	×	×	√
This study	√	√	√	√

Table 7. Comparison of encryption modes.

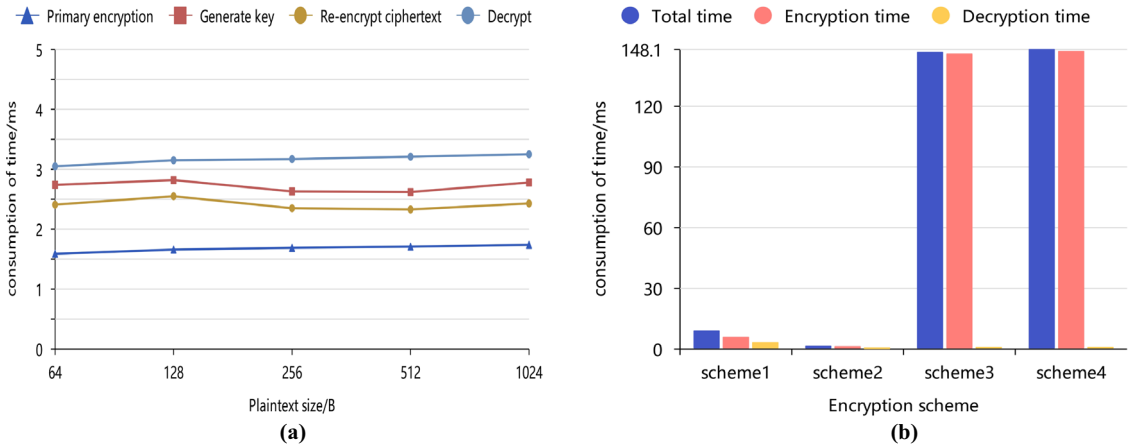


Fig. 14. Agricultural blockchain BBPR-AC proxy re-encryption performance test. (**a**) BBPR-AC Proxy re-encryption consumes time in each phase (**b**) Performance Comparison of Encryption Methods.

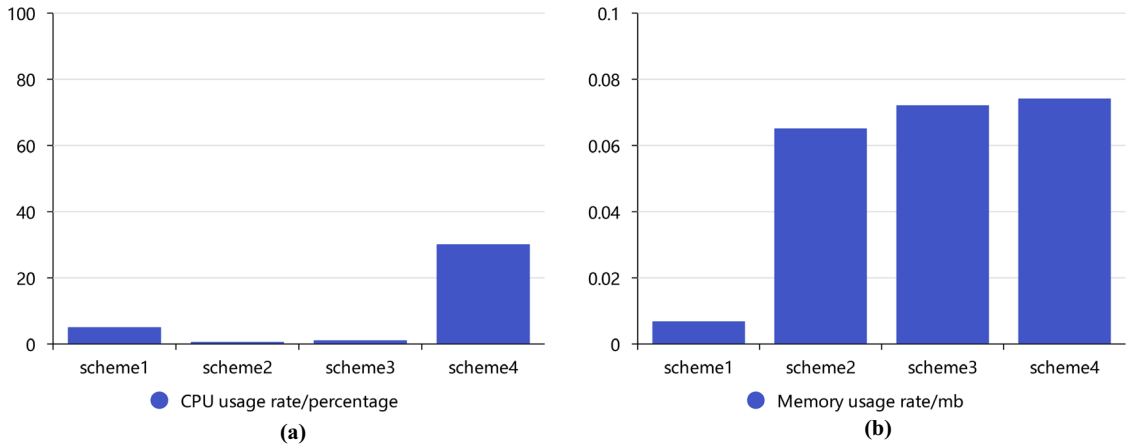


Fig. 15. BBPR-AC agent re-encryption resource consumption test. (**a**) BBPR-AC Proxy re-encryption CPU usage rate (**b**) BBPR-AC Proxy re-encryption Memory usage rate.

Characterisation	Jianbiao et al.[34]	Gechang et al.[35]	Wenjun et al.[36]	Wang et al.[37]	This study
Blockchain-based	√	√	√	×	√
fine-grained access control	√	×	√	√	√
privacy protection	√	√	√	√	√
Support for property update	√	×	×	√	√
Data tampering prevention	√	×	√	√	√
smart contract	√	×	×	×	√

Table 8. Comparison of access control modes.

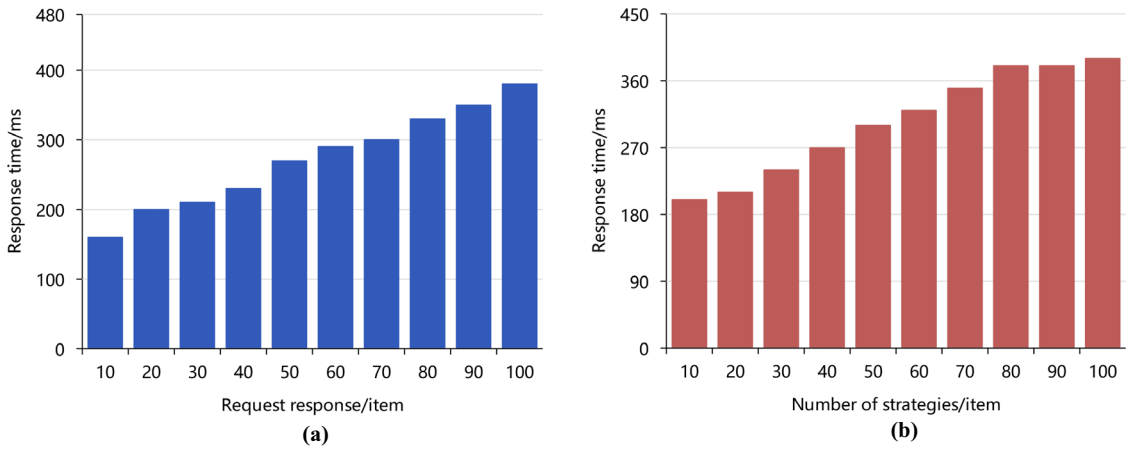


Fig. 16. Request and policy response times. (**a**) Request Response Time (**b**) Strategy judgment time.

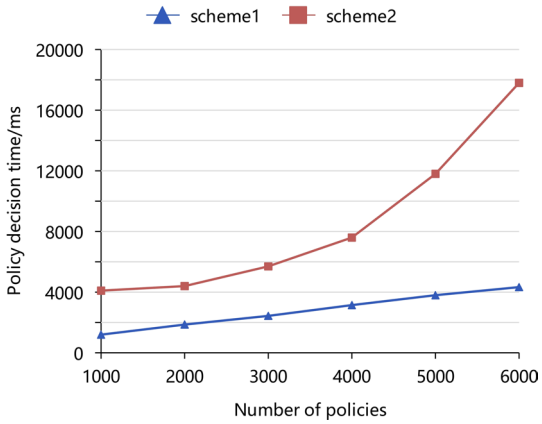


Fig. 17. BBPE-AC Policy decision time.

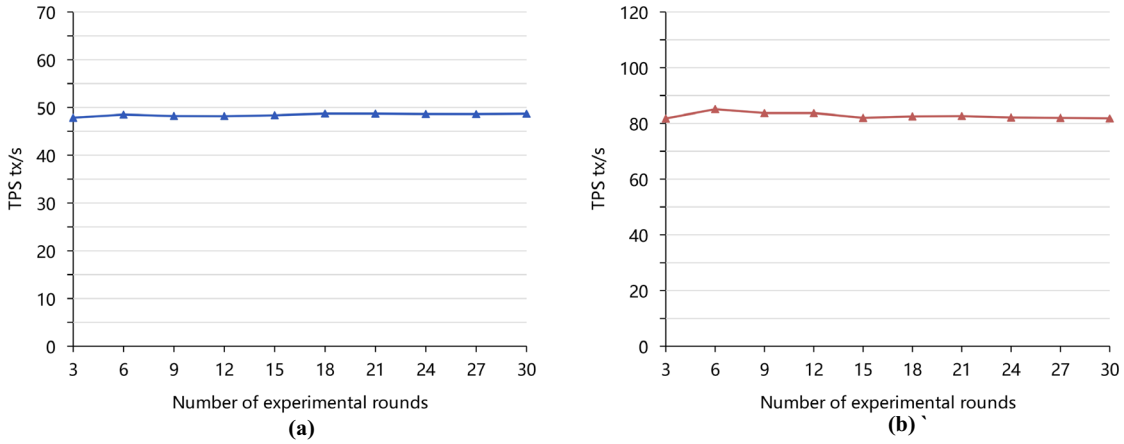


Fig. 18. Agricultural products traceability blockchain performance test. (**a**) Biological risk factor data upload throughput (**b**) Biological risk factor data query throughput.

Data availability

The datasets generated and/or analysed during the current study are not publicly available for security reasons, but are available from the first author, shaohua wang, upon reasonable request.

Received: 18 June 2024; Accepted: 19 August 2024
Published online: 29 August 2024

References

1. Bian, X., Yao, G. & Shi, G. Social and natural risk factor correlation in China's fresh agricultural product supply. *PLoS ONE* **15**, e0232836. https://doi.org/10.1371/journal.pone.0232836 (2020).
2. Li, P.-C., Shih, H.-C. & Ma, H.-W. Assessing the transfer of risk due to transportation of agricultural products. *Chemosphere* **120**, 706–713. https://doi.org/10.1016/j.chemosphere.2014.10.009 (2015).
3. Dai, M. & Liu, L. Risk assessment of agricultural supermarket supply chain in big data environment. *Sustain. Comput. Inf. Syst.* **28**, 100420. https://doi.org/10.1016/j.suscom.2020.100420 (2020).
4. Tong, J. *et al.* Pesticide residue and dietary intake risk of vegetables grown in Shanghai under modern urban agriculture in 2018–2021. *Heliyon* **10**, e25505. https://doi.org/10.1016/j.heliyon.2024.e25505 (2024).
5. Linlin, X., Shuang, Q., Ruotong, W., Ruyu, L. & Xiaohua, L. Spatiotemporal trends of foodborne disease outbreaks in China from 2011 to 2020. *Health Res.* **52**, 226–231. https://doi.org/10.19813/j.cnki.weishengyanjiu.2023.02.009 (2023).
6. Khan, M. A. & Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst. Int. J. Escience* **82**, 395–411. https://doi.org/10.1016/j.future.2017.11.022 (2018).
7. Galvez, J. F., Mejuto, J. C. & Simal-Gandara, J. Future challenges on the use of blockchain for food traceability analysis. *TRAC-Trends Anal. Chem.* **107**, 222–232. https://doi.org/10.1016/j.trac.2018.08.011 (2018).
8. Liu, W., Shao, X. F., Wu, C. H. & Qiao, P. A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development. *J. Clean. Prod.* **2021**, 298. https://doi.org/10.1016/j.jclepro.2021.126763 (2021).

9. Ogunseyi, T. B., Avoussoukpo, C. B. & Jiang, Y. A systematic review of privacy techniques in recommendation systems. *Int. J. Inf. Secur.* **22**, 1651–1664. https://doi.org/10.1007/s10207-023-00710-1 (2023).
10. Alloghani, M. *et al.* A systematic review on the status and progress of homomorphic encryption technologies. *J. Inf. Secur. Appl.* **48**, 102362. https://doi.org/10.1016/j.jisa.2019.102362 (2019).
11. Meliana, C., Liu, J., Show, P. L. & Low, S. S. Biosensor in smart food traceability system for food safety and security. *Bioengineered* **15**, 2310908. https://doi.org/10.1080/21655979.2024.2310908 (2024).
12. Darbandi, M. *et al.* Blockchain systems in embedded internet of things: Systematic literature review, challenges analysis, and future direction suggestions. *Electronics* **11**, 4020. https://doi.org/10.3390/electronics11234020 (2022).
13. Mishra, R., Ramesh, D., Mohammad, N. & Mondal, B. Blockchain enabled secure pharmaceutical supply chain framework with traceability: An efficient searchable pharmachain approach. *Cluster Comput.* https://doi.org/10.1007/s10586-024-04626-w (2024).
14. Mishra, R., Ramesh, D., Edla, D. R. & Qi, L. VaccineChain: A checkpoint assisted scalable blockchain based secure vaccine supply chain with selective revocation. *J. Ind. Inf. Integr.* **34**, 100485. https://doi.org/10.1016/j.jii.2023.100485 (2023).
15. Li, C., Lu, Y. X., Bian, Y., Tian, J. & Yuan, M. Design of safety evaluation and risk traceability system for agricultural product quality. *Appl. Sci.-Basel* **2024**, 14. https://doi.org/10.3390/app14072980 (2024).
16. Salah, K., Nizamuddin, N., Jayaraman, R. & Omar, M. Blockchain-based soybean traceability in agricultural supply chain. *IEEE ACCESS* **7**, 73295–73305. https://doi.org/10.1109/ACCESS.2019.2918000 (2019).
17. Alshehri, D. M. Blockchain-assisted internet of things framework in smart livestock farming. *Internet of Things* **22**, 100739. https://doi.org/10.1016/j.iot.2023.100739 (2023).
18. Khanna, A., Jain, S., Burgio, A., Bolshev, V. & Panchenko, V. Blockchain-enabled supply chain platform for Indian dairy industry: Safety and traceability. *Foods* **11**, 2716. https://doi.org/10.3390/foods11172716 (2022).
19. Peng, X. *et al.* Construction of rice supply chain supervision model driven by blockchain smart contract. *Sci. Rep.* **12**, 20984. https://doi.org/10.1038/s41598-022-25559-7 (2022).
20. Yao, Q. & Zhang, H. Improving agricultural product traceability using blockchain. *Sensors* **22**, 3388. https://doi.org/10.3390/s22093388 (2022).
21. Guan, S., Wang, Z. & Cao, Y. A novel blockchain-based model for agricultural product traceability system. *IEEE Commun. Mag.* **61**, 124–129. https://doi.org/10.1109/MCOM.002.2200815 (2023).
22. Kim, J. *et al.* Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption. *Annu. Rev. Control* **54**, 200–218. https://doi.org/10.1016/j.arcontrol.2022.10.002 (2022).
23. Lu, S., Zheng, J., Cao, Z., Wang, Y. & Gu, C. A survey on cryptographic techniques for protecting big data security: Present and forthcoming. *Sci. China Inf. Sci.* **65**, 201301. https://doi.org/10.1007/s11432-021-3393-x (2022).
24. Keshta, I. *et al.* Blockchain aware proxy re-encryption algorithm-based data sharing scheme. *Phys. Commun.* **58**, 102048. https://doi.org/10.1016/j.phycom.2023.102048 (2023).
25. Song, J. *et al.* Proxy re-encryption-based traceability and sharing mechanism of the power material data in blockchain environment. *Energies* **15**, 2570. https://doi.org/10.3390/en15072570 (2022).
26. Agyekum, K.O.-B.O. *et al.* A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Syst. J.* **16**, 1685–1696. https://doi.org/10.1109/JSYST.2021.3076759 (2021).
27. Pal, S., Dorri, A. & Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. *J. Netw. Comput. Appl.* **203**, 103371. https://doi.org/10.1016/j.jnca.2022.103371 (2022).
28. Servos, D. & Osborn, S. L. Current research and open problems in attribute-based access control. *Assoc. Comput. Mach.* **49**, 4. https://doi.org/10.1145/3007204 (2017).
29. Aodi, L., Xuehui, D., Na, W. & Shaozhuo, L. Blockchain-based big data access control mechanism. *J. Softw.* **30**, 2636–2654. https://doi.org/10.13328/j.cnki.jos.005771 (2019).
30. Xuan, H. & Mengling, Y. Ring secret transaction protocol based on multivariable public key cryptosystem. *Comput. Sci.* **50**, 756–761. https://doi.org/10.11896/jsjkx.220100157 (2023).
31. Youliang, T., Yang, C., Zuan, W. & Tao, F. Blockchain data traceability algorithm based on attribute encryption. *J. Commun.* **40**, 101–111. https://doi.org/10.11959/j.issn.1000-436x.2019222 (2019).
32. Feng, T., Pei, H., Ma, R., Tian, Y. & Feng, X. J. Blockchain data privacy access control based on searchable attribute encryption. *Comput. Mater. Continua* **66**, 871–890. https://doi.org/10.32604/cmc.2020.012146 (2021).
33. Khan, M. Y., Zuhairi, M. F., Ali, T., Alghamdi, T. & Marmolejo-Saucedo, J. A. J. W. N. An extended access control model for permissioned blockchain frameworks. *Wirel. Netw.* **26**, 4943–4954. https://doi.org/10.1007/s11276-019-01968-x (2020).
34. Jianbiao, Z., Zhaoqian, Z., Wanshan, X. & Na, W. An inter-domain access control model based on blockchain. *J. Softw.* **32**, 1547–1564. https://doi.org/10.13328/j.cnki.jos.006011 (2021).
35. Gechang, L. & Qiang, L. Blockchain data privacy protection mechanism based on searchable encryption. *Comput. Appl.* **39**, 140–146 (2019).
36. Wenjun, L., Shenglian, W. & Yu, C. Blockchain-based electronic medical record sharing solution. *Comput. Appl.* **40**, 157–161. https://doi.org/10.11772/j.issn.1001-9081.2019060994 (2020).
37. Wang, S., Yao, L., Chen, J. & Zhang, Y. J. I. A. KS-ABESwET: A keyword searchable attribute-based encryption scheme with equality test in the internet of things. *IEEE Access* **7**, 80675–80696. https://doi.org/10.1109/ACCESS.2019.2922646 (2019).

Acknowledgements

This work was funded by National Key Research and Development Plan Project (2023YFF0614404): Construction and application of biological risk traceability platform for important primary agricultural products and supported by Jiangsu Province Science and Technology Plan (Key Research and Development Plan Modern Agriculture) Project (BE2023315): Research and application demonstration of key technologies of intelligent supply chain of fresh agricultural products e-commerce.

Author contributions

Shaohua Wang: Paper conception, Blockchain part implementation, System design, System testing, Draft preparation, Data curation, Formal analysis. Chuanheng Sun: Funding acquisition, System framework propose, Formal analysis. Na Luo: Paper conception, Methodology, Formal analysis. Bin Xing: Paper conception, Formal analysis. Zhenzhen Sun: Paper conception. Hang Zhang: Paper conception.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.Z. or C.S.