Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070710
ISSN 2371-8838 Vol. 7 Num. 7

Design and Implementation of Beef Product Quality and Safety Traceability System Based on Blockchain Technology

Xin Tang*, Wen Chen, Zhi Mou, Zhilan Ji

College of Management Science, Chengdu University of Technology, Chengdu, Sichuan, China
**Corresponding author*

Keywords: Traceability, consortium blockchain, beef products, multi-level association retrieval

Abstract: With the progress of society, the society pays more attention to food safety, and the demands of consumers and regulatory authorities also increase. The original beef traceability system seems to be unable to meet the demand because of the complicated traceability links, difficult traceability and easy tampering of node data. In order to better meet the needs of the public, a beef product traceability system based on blockchain is designed. The core board is mainly based on consensus algorithm to package data on the chain and update the latest block height, and then use hash function to encrypt the information data on the chain, and then use the node-association-based hash matching retrieval and verification method to provide feedback verification of the obtained results, thus realizing the real and comprehensive, efficient and safe multi-level deep traceability of the whole beef cattle supply chain system, effectively guaranteeing the depth, breadth and credibility of traceability information. It effectively guarantees the depth, breadth and credibility of traceability information, and has good practical application prospects compared with traditional traceability systems.

1. Introduction

Traditional beef product safety traceability systems have achieved some degree of food traceability through methods such as QR codes and radio frequency identification technology [1]. However, the centralized management mode used by traditional traceability systems may lead to the following issues: (1) poor data quality due to different data sources, non-standard data entry, and inconsistent data standards; (2) difficulties in ensuring data authenticity, as the traceability system lacks government supervision and management, providing opportunities for some intentionally fraudulent enterprises to replace and tamper with quality and safety information data; (3) excessive system development costs due to the need for technical, human, and material costs, resulting in high system development costs [2].

With the continuous development of blockchain technology, a trustworthy and complete supply chain based on consortium chains has the advantages of decentralization, transparency, efficiency, low cost, and traceability, which can better achieve low-cost, multi-level association traceability for

the entire process. This provides more reliable data for regulatory authorities and consumers to comprehensively trace and supervise the quality and safety of beef products [3,4].

This article combines traditional traceability systems with blockchain technology to solve the problems of data collection, data authenticity, and cost in traditional food safety traceability systems. It improves the reliability, security, and efficiency of the system and provides powerful technical support for the quality and safety guarantee of beef products.

2. Overview of Blockchain

Blockchain is a decentralized digital ledger technology that enables secure, transparent and immutable transactions between parties without the need for a centralized authority. It is a peer-to-peer network that allows multiple parties to access, validate, and record transactions in a secure and transparent way.

One of the key features of blockchain is its distributed storage technology. In a blockchain network, every participant has a copy of the ledger, which is constantly updated and verified by other nodes in the network. This ensures that the data is decentralized, tamper-proof and resistant to hacking attacks [5,6].

Another important feature of blockchain is the block timestamp, which is a unique identifier that marks the time when a block is added to the blockchain [7,8]. This timestamp is generated by a consensus mechanism, such as proof of work or proof of stake, which ensures that the blocks are added to the blockchain in a secure and transparent manner [9,10].

Alliance chain technology is a variation of blockchain that allows multiple organizations to collaborate and share data on a private and permissioned network [11,12]. This type of blockchain is ideal for enterprises that require a higher level of privacy and security for their transactions [13,14].

Data retrieval on the chain is also a key aspect of blockchain technology. Because the data is stored in a decentralized manner, it can be retrieved by anyone with access to the network. This makes it easy to trace the history of transactions and to verify the authenticity of data [15].

In summary, blockchain technology have a range of features and benefits that make it ideal for a wide variety of applications, including distributed storage, secure and transparent transactions, and data retrieval. Blockchain technology has become an increasingly valuable tool for enterprises and organizations all over the world.

3. Design Proposal for Beef Traceability System

3.1. Functional Module Design for Traceability System

The construction of the beef traceability system model is roughly divided into four modules: consortium chain member management, enterprise data recording and management, data encryption for on-chain upload, and multi-level association retrieval and verification. The technical scheme flow of product deep traceability is shown in Figure 1.

The consortium chain member management module activates permissions for node members according to identity level gradient rules, combining information data circulation and efficiency. The enterprise data recording and management module inputs and manages traceability information, and its flexibility is reflected in its ability to transmit data to the blockchain on an independent platform.

The data encryption for on-chain upload module mainly uses the core consensus algorithm to determine matching results and create encrypted blocks, allowing users to efficiently access traceability data results through digital certificates. The multi-level association retrieval and verification module fully utilizes hash algorithms to derive the hash value of the traceability code. By analyzing the core node attributes and relevant node attributes separately, it achieves fast matching

verification of the hash value.

3.2. Member Management of Alliance Chain

The "Alliance Chain" Member Management Platform is used to enter the basic information of registered members and establish the node properties corresponding to their identities. These identity properties should be roughly divided into: breeding households or breeding enterprises, beef product processing enterprises, consumers, quality inspectors, traceability system enterprises, system administrators, and transportation enterprises. Then, the administrators on the alliance chain assign different weight levels to each member according to the weight gradient previously formulated based on actual conditions. Finally, based on the registered identity node properties and weight, the differential permissions of the alliance chain nodes are authorized and activated.

For the entire beef supply chain traceability system from breeding to purchase, the completed supply chain system involves the participation of multiple organizations such as producers, traceability enterprises, regulators, and consumers, forming a typical "alliance chain" application scenario. Traditional traceability technologies represented by QR codes, barcodes, and RFID radio frequency technology save the data collected by each link in the database of the central node with limited access rights in a highly "centralized" form, which not only poses the problem of unclear responsibility for food safety issues due to highly dispersed links, but also poses serious consequences of a new round of trust crises caused by the high risk of product supply chain information being often non-transparent and core data being tampered with. Therefore, the design of the beef traceability system using "alliance chain technology" aims to simplify the traditional traceability process by utilizing the advantage of accurate diagnosis of traceability problems to solve the trust crisis caused by the information asymmetry between production parties, sales vendors, government, and consumers under the traditional solution.

"Alliance chain technology" as a branch under the background of blockchain integrates the advantages of blockchain technology-based traceability system design, realizes "decentralization" of data storage and management, avoids manipulation and tampering of data by various nodes, and guarantees data security and credibility. At the same time, the "Alliance chain" consists of several nodes represented by a few relatively fixed organizations or individuals after authorization, which ensures that data in the beef traceability system, including enterprise trade secrets and personal privacy, can only flow between a few relatively fixed members. In addition, the "Alliance Chain technology" adopts privacy policies of encryption algorithms and permission control, which not only reduces the risks of data leakage and privacy disclosure that may be caused by "public chain technology", but also greatly avoids the problem of data closure and difficulty in sharing caused by "private chain technology".

3.3. Enterprise Data Recording and Management

This section is based on the "Enterprise Application End" to complete its function as the data collection and storage entity for the cattle traceability system. The data is collected in sequence, starting with the employee information of the beef product company, the company's main and related information, product sales information, product transportation and warehousing information, enterprise financial information, and the data of the affiliated enterprise link of the traceability code system. Then, the information on the breeding site and daily breeding mode of cattle, basic information of the cattle breeding and slaughter supply chain, cattle health information and inspection, and beef product production line processing and packaging information are gathered. The aim is to establish a complete product traceability information system based on a sound traceability enterprise link. Finally, the traceability system automatically generates traceability codes based on the traceable

information above.

3.4. Data On-chain Encryption

The "Alliance Chain Management Platform" and the "Enterprise Application End" are the two major operating applications for the "Data On-Chain Encryption" section. The specific technical solution is as follows:

$$\frac{Hash(K_{pub},Hash_{pb})}{B_e} < D_{cb} \times (T_{cur} - T_{pb}) \quad (1)$$

(1) The data to be put on the chain collected by the previous section will be marked. The mark should include information such as the first and last node properties of data transmission, data summary, data type, data collection time, and data collection party. (2) Based on the Proof of Stake (Pos) consensus algorithm, the alliance chain consensus algorithm will integrate and package the data before putting it on the chain, and then update the latest block height. The core formula is that the numerator hash function in the left-hand side of the inequality represents the account public key and the previous block hash value respectively, and the denominator represents the available balance of the account. The right-hand side of the inequality is the current block difficulty coefficient, the current time, and the time the previous block was generated, respectively. Only when the latest block height value satisfies this inequality can the complete establishment of a new block be ensured. (3) Use a hash algorithm with a hash function as the core to encrypt the data to be put on the chain. The core formula is: h = H(M), where "H(M)" is a fixed-length bit string, and "M" is a message string of any length. It is mainly used to generate block addresses, equity proof calculations, and other aspects. (4) Issue valid digital certificates to alliance chain members who have been authorized by the system administrator, which can be used to read on-chain data and verify identities.

3.5. Multi-level Associative Retrieval and Verification

This section includes three operation ports: the "Enterprise Application Side," the "Deep Traceability Consumer Query Side," and the "Traceability Supervision Platform." The technical scheme is shown in figure 2, and its principle is explained as follows:

Firstly, there is the hash matching retrieval and verification method, which is a retrieval and verification method based on node correlation. The initial traceability information obtained from the first query is called the primary traceability information, and the associated traceability information obtained from the second query to any subsequent queries is called the secondary traceability information. This retrieval and verification method is executed in six steps: (1) retrieve the target block corresponding to the hash value of the primary traceability information; (2) use the matching target block obtained in the previous step as the CORE node; (3) find all RELATED nodes along the node attribute corresponding to the CORE node. For example, if the CORE node A is the seller of product α, then the RELATED nodes of A will include the producer β, the transporter γ, and even the producer δ of the raw materials. The attribute of the CORE node not only includes the supply relationship between nodes but also covers the degree of relatedness of the production relationship. In the above example, the producer has the highest degree of relatedness with the seller, not the transporter, and the producer has the highest degree of relatedness with the raw material producer, not the seller. Therefore, the entire alliance chain operation system calculates the correlation between nodes based on the degree of relatedness of the above node attributes. (4) The formation of a new block must be accompanied by the creation of a new timestamp, and each node will generate a block containing the on-chain traceability information. Therefore, by arranging the hash values of these numerous timestamps in the natural chronological order, a historical traceability data archive table

can be obtained. Similarly, a set of historical traceability data archive tables composed of all associated nodes of a core node can be obtained. (5) According to the chronological order of the transaction contract, a block pool of on-chain traceability information hash values to be matched can be formed by sorting the obtained historical traceability data archive tables. (6) The method of verifying whether the matching is successful is to compare the hash value in the block pool corresponding to the traceability information query for the related input or output products of the next level initiated by the system user with the hash value of the original record data. If a matching equal hash value is found, the matching is successful; if not, the matching fails. Finally, the verification result is obtained. Then, each time all steps are fully executed and the final matching verification result is obtained, the traceability code reading and statistical accumulation update will be implemented, and the record data corresponding to the traceability code will also be refreshed in real time. Finally, each time a traceability query with a final matching verification result is completed, a traceability query record containing the data obtained by the user completing the traceability query will be created, and it will be automatically pushed to the traceability supervision platform.

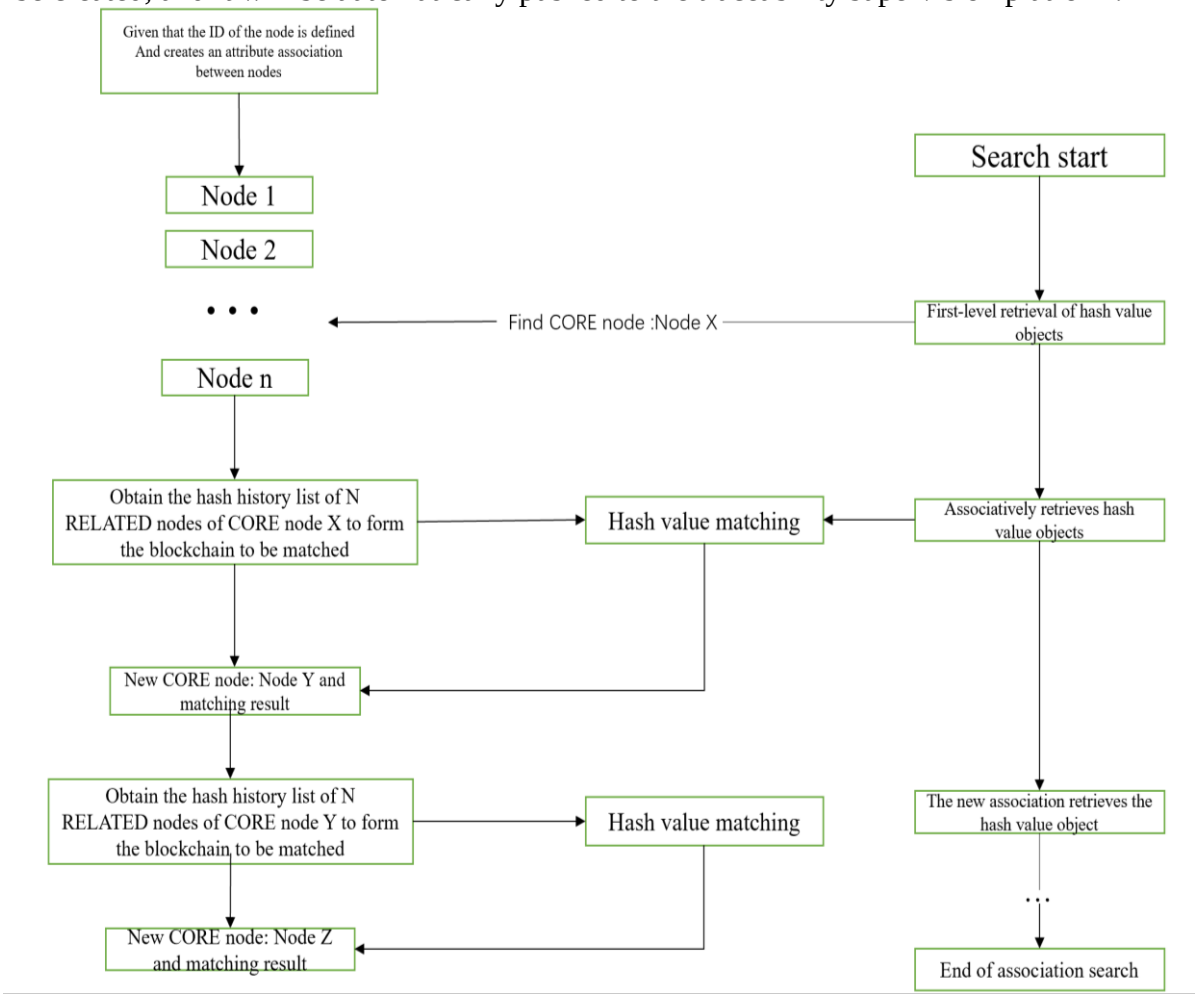

Figure 1: Technical flow chart of product traceability system

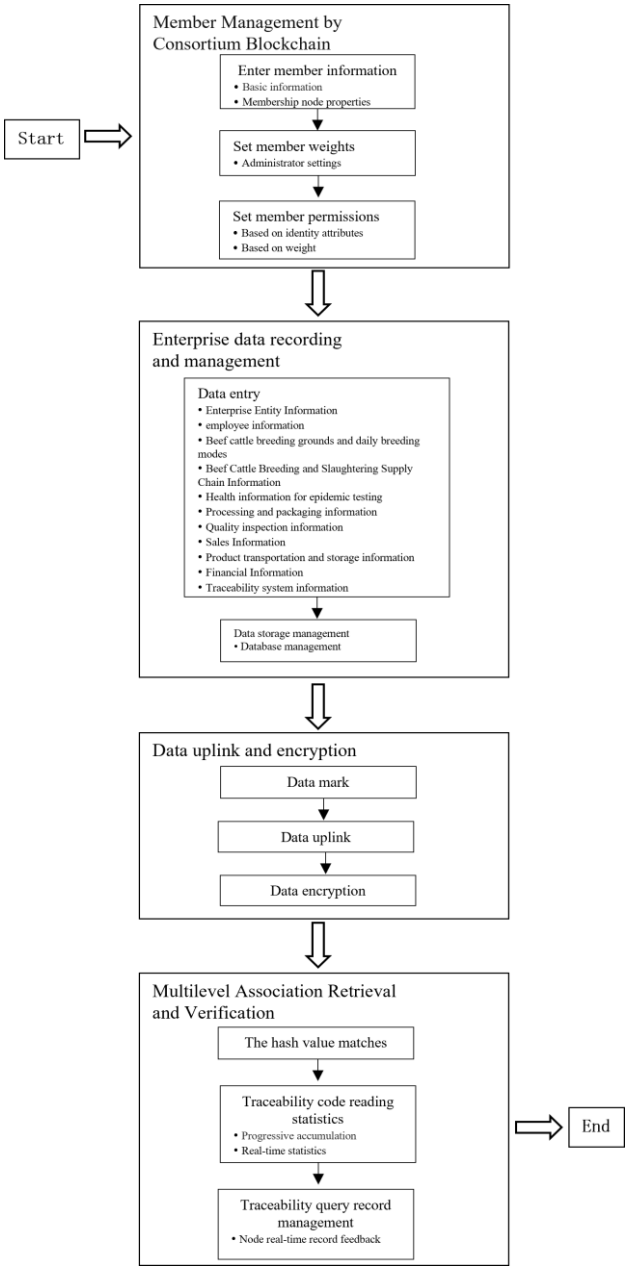

Figure 2: Beef product depth traceability system design flowchart

4. System Application Implementation Scheme and Result Analysis

Assume that the existing beef breeding enterprise A, beef slaughtering enterprise B, transportation enterprise C, distribution enterprise D and supervision department E 5 entities join the system for management, and the specific implementation scheme is as follows:

Initially, five entities want to join the alliance chain, and they need to submit a registration application to the traceability system enterprise to achieve this goal. When applying, you need to provide basic information and subject attributes, such as breeding enterprises, slaughtering enterprises, transportation enterprises, distribution enterprises, regulatory authorities, etc. The system will review the information provided by combining automation and manual review. If approved, the traceability system enterprise will create an account for the relevant entity enterprise, activate it, and assign it a unique number. Based on its identity attribute, the system will also set the corresponding

governance weight level and authorize the corresponding functional authority in the chain.

Each entity enterprise has its own enterprise administrator, namely, subject A, subject B, subject C and subject D. These administrators are responsible for adding the accounts of the recorder, and each account corresponds to a recorder, and assigning permissions to them. Administrators need to update account information regularly, including account number, password, recorder name and role. The administrator should also set up a personnel management page to display the basic information of the recorder, such as employee ID, enterprise code, employee account number, telephone number, role and name. Administrators can only manage and view the information of their own enterprises. Enterprises can decide data sharing through negotiation, and the scope and depth of sharing are decided by enterprises themselves.

Each recorder in subject A, subject B, subject C and subject D enters the information of beef food production into their internal database according to their assigned authority, and the enterprise administrator can only view the information of each link of pork supply chain and cannot modify it. After the recorder uploads the information, the enterprise administrator only needs to mark the data and apply for data uploading. After the data uploading, the system encrypts the data into non-plaintext string data through hash encryption algorithm.

Because the information in the process of beef food production has been uploaded and cannot be tampered with, when supervising the safety production of beef products, the supervision department E can submit an application for inquiring the relevant data of the supervised subject to the system. The system will verify the identities of the supervision unit and the supervised subject. After the verification, the supervision department can obtain higher authority to obtain data, and the system will automatically generate corresponding reports or traceability information to access the details of beef from breeding to sales, so as to determine the source of the problem and formulate corresponding accountability measures.

Consumers can directly access the traceability inquiry website of the system, input the traceability code on the product or scan the traceability QR code on the product to deeply trace the product. It includes beef production timeline (including birth, slaughter, quarantine, slaughter, processing and other stages, and the number of the recorder), product information (including beef product type, sales price, sales point, production date, etc.), product details (including breeding unit information, slaughter enterprise information, quarantine information, transportation information, etc.). The data is authentic and has not been tampered with, which can reassure consumers and promote the healthy development of enterprises in the beef product supply alliance chain.

5. Summary

To sum up, the system can not only trace the whole process of beef products in production through blockchain technology, but also ensure the data security of the enterprise itself. Moreover, after the beef products have problems, the regulatory authorities and consumers can quickly and accurately pursue them, thus fully protecting the rights and interests of consumers.

Compared with the traditional beef product quality and safety traceability system, the main advantages of this system are summarized as follows: (1) The important business data of all institutions on the system are trusted, encrypted and highly secure, and these data are only shared among members in the blockchain, and it is not easy for others to steal important data through network attacks such as traceability queries from regulatory authorities or consumers. (2) The regulatory authorities or consumers can easily obtain the production, processing, storage and other information of beef products through multiple means of traceability, and realize efficient multi-level related traceability query, so as to realize the whole traceability of products. (3) Because once the data is uploaded, it can't be changed, and the system will monitor the data in real time, and it will immediately

report to the police once an abnormal value is found, so once the beef quality and safety incident occurs, the system can be completely trusted, and the problem link can be traced back quickly according to the system, and the responsible enterprise will be punished and required to rectify. The application of this system can promote the sustainable development of the whole industry, and also form the industry atmosphere of honest management.

At the same time, we also realize that we can optimize the system in the following aspects in the future: (1) Put the system into practical application, verify the actual effect and advantages of the system, and constantly optimize the system through user feedback, so that it can meet the needs of users as much as possible. (2) Optimize the terminal for obtaining traceability data, and take automatic data winding instead of manual data entry, so as to increase the credibility of traceability information and reduce the cost of information entry. (3) Further optimize the data winding and data retrieval algorithm, improve the speed of tracing data winding and improve the efficiency and accuracy of tracing information retrieva.

Acknowledgement

This work is sponsored by National Undergraduate on Innovation and Entrepreneurship Project, No. 202210616013.

References

[1] Wu X., Zhan X., & Hu J. (2021). Design and implementation of food safety traceability system based on RFID and QR code. Journal of Science of Teachers' College and University, (01), 32-35+55.
[2] Lu R., Wang Z., Li L., & Wang J. (2020). A Scheme about Agricultural Produce Traceability Using Blockchain Based on Hyperledger Fabric. Computer Science and Application, 10 (5), 811-823.
[3] Wu J., Du C., Ma Z., & Zheng G. (2019). Blockchain Architecture Design for Food Traceability System. Computer Applications and Software, (12), 46-50+86.
[4] Chen N., Shen K., & Liang C. (2021). Hybrid Decision Model for Evaluating Blockchain Business Strategy: A Bank's Perspective. Sustainability, 13 (11), 5809. https://doi.org/10.3390/su13115809.
[5] Duan H., & Bi L., (2021). Research on Distributed Storage Technology of Database Big Data Based on Cloud Computing. Journal of Physics: Conference Series, 1982 (1), 012195. doi:10.1088/1742-6596/1982/1/012195.
[6] Cangir O., Cankur O., & Ozsoy A. (2021). A taxonomy for Blockchain based distributed storage technologies. Information Processing and Management, 58 (5), 102627. doi:10.1016/J.IPM.2021.102627.
[7] Ma G. (2020). Research on Reliable Timestamp Service Mechanism of Bitcoin Platform (Master's Degree Thesis, Nanjing University of Aeronautics and Astronautics). Retrieved from https://kns.cnki. net/kcms/ detail/detail. aspx? dbname=CMFD202102&filename=1021592189.nh.
[8] Huang D., & Li K. (2023). Research on Multi-address Time-based Blockchain Covert Communication Method. Journal on Communications, (02), 148-159.
[9] Estevam G., Palma L. M., Luan R. S., Martina J. E., & Vigil M. (2021). Accurate and decentralized timestamping using smart contracts on the ethereum blockchain. Information Processing & Management, 58, 102471.
[10] Jaquet-Chiffelle D., Casey E., & Bourquenoud J. (2022). Corrigendum to 'tamperproof timestamped provenance ledger using blockchain technology' [forens. sci. int.: digit. invest. 33 (2020) 300977]. Forensic Science International: Digital Investigation, 40.
[11] Ma X. (2018). Blockchain based supply-chain finance service platform. Big Data Research, 4 (1), 2018002. doi:10.11959/j.issn.2096-0271.2018002.
[12] Gao W., Mu W., Huang S., Wang M., & Li X. (2021). Improved Byzantine Fault-Tolerant Algorithm Based on Alliance Chain. Wireless Communications and Mobile Computing. doi:10.1155/2021/8455180.
[13] Jiang W., Wu X., Song M., Qin J., & Jia Z. (2023). A Scalable Byzantine Fault Tolerance Algorithm Based on a Tree Topology Network. IEEE Access, 33509-33519. doi:10.1109/ACCESS. 2023.3264011.
[14] Chen Y., Li M., Zhu X., Fang K., Ren Q., Guo T., ... & Deng Y. (2022). An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain. Information Processing and Management, 59 (2), 102884. doi: 10. 1016/J. IPM. 2022.102884.
[15] Zhang D. (2022). Research on Efficient Retrieval on Blockchain Based on Distributed Storage. Xidian University. Retrieved from https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFDTEMP&filename=1023023618.nh.