2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA) | 978-1-6654-2877-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICIBA52610.2021.9687951

# Design of college student information sharing system based on blockchain

Peng Jiang[1,2], Yanhui Feng[1,2] , Yonghui Dai[3*]
1. Jingan Branch Campus, Shanghai Open University, Shanghai, China
2. Shanghai JingAn District College, Shanghai, China
3. School of Management, Shanghai University of International Business and Economics, Shanghai, China
jzhpmail@163.com, fengyanhui@hotmail.com, daiyonghui@suibe.edu.cn
Corresponding Author: Yonghui Dai Email: daiyonghui@suibe.edu.cn

***Abstract*—College Students information sharing is of great significance for college students' employment and enterprise recruitment, and it can improve the recruitment efficiency. As blockchain technology has been gradually applied to the sharing system in many fields, this paper presents the design of college student information system based on blockchain, which mainly including system architecture and main process design, as well as key technologies such as consensus algorithm and smart contract deployment. The system has good security and traceability, and provides a new idea for college students' information sharing.**

***Keywords—Sharing system; blockchain technology; college student system; smart contract***

## I. Introduction

In recent years, the development of computer technology has continuously improved the information management level of universities, and various types of information data of college students have become more and more detailed. By analyzing the data of college students such as academic record, physical quality, reward and punishment data, we can well grasp the situation of college students, which is very important for college student management and enterprise recruitment. However, because the lack of sharing of student information in many colleges and universities at present, the student data can only be checked by the university to which it belongs, and the value of the data cannot be fully utilized. The main reason for the above phenomenon is that data sharing needs to solve some problems, such as data security and traceability. If a college student's academic record has been tampered with, it needs to be traced back to who made the tampering. The traditional college student information management system is difficult to achieve the above objectives. Considering that blockchain technology has the characteristics of decentralization and tamper proof, it is very suitable for the realization of college students' information sharing.

Blockchain is a typical distributed system based on peer-to-peer network. The network is jointly maintained by all nodes [1]. It uses cryptographic algorithms to ensure the security of data transmission and access, uses distributed ledger to verify and store data, and executes contracts through intelligent contract mechanism [2][3]. The data can only be added and cannot be deleted or tampered with, which ensures the traceability of the data from the algorithm level.

## II. Literature Review

Blockchain technology originated from Bitcoin. It combines existing theoretical solutions and its own technological innovations to bring disruptive changes in the digital currency market, and it has been widely used in finance, taxation, certification and government management. From a technical point of view, blockchain technology is closely related to cryptography, especially elliptic curve cryptography occupies an important position in cryptographic research. It is an encryption form combining elliptic curve and public key cryptosystem to achieve the purpose of security [4]. After that, some researchers proposed a zero-knowledge proof method based on cryptography. The essence of this method is to maintain the digital currency ledger based on network users. While maintaining the ledger, it can keep the participants' information confidential, so as to realize the anonymity of participants and users [5]. In the research of blockchain, some scholars have studied smart contracts and consensus algorithm. For example, Sillaber (2017) et al studied the distributed ledger of blockchain from the perspective of life cycle, and analyzed the bookkeeping characteristics of each stage [6]. Thai (2019) et al studied the consensus algorithm, they improved the Byzantine algorithm with the idea of layering, and solved the problem of capacity expansion of Byzantine fault-tolerant protocol [7].

In the research of information sharing, some scholars have conducted application research in different fields based on blockchain. For example, Ren (2018) et al studied the application of blockchain technology in government management, analyzed whether blockchain technology can help the government carry out process innovation and transformation in e-government, and gave suggestions for management process improvement based on blockchain technology [8]. Fanning (2016) et al studied the application of blockchain in the field of financial services, They believe that the data record of blockchain is not only a distributed database, but also has the characteristics of decentralization, openness, and tamper resistance. It can be used to record the balance of accounts and is secure [9]. Balis (2019) et al studied the hospital data sharing based on blockchain, gave the overall architecture and authentication process, and realized the safe transmission and sharing of data [10].

## III. System design

### A. System architecture

The purpose of student information sharing system is to establish a safe and reliable information query and storage system. The first consideration of the system is the storage of data. How to store data safely is a problem that must be considered in data sharing. Secondly, the system should consider the access of data. How to provide convenient and safe access to the outside world and ensure the security of data while providing good services to the outside world is a problem to be solved in the system design. In addition, the system also needs to consider the smart contract consensus in the blockchain network. How to design a reasonable smart contract consensus mechanism and optimize service performance is also a problem that the system needs to solve. Therefore, the system uses distributed and decentralized storage of college students' information data. Its main functions include data chaining, data maintenance, information query authorization, etc. Blockchain system architecture is shown as in Fig. 1.

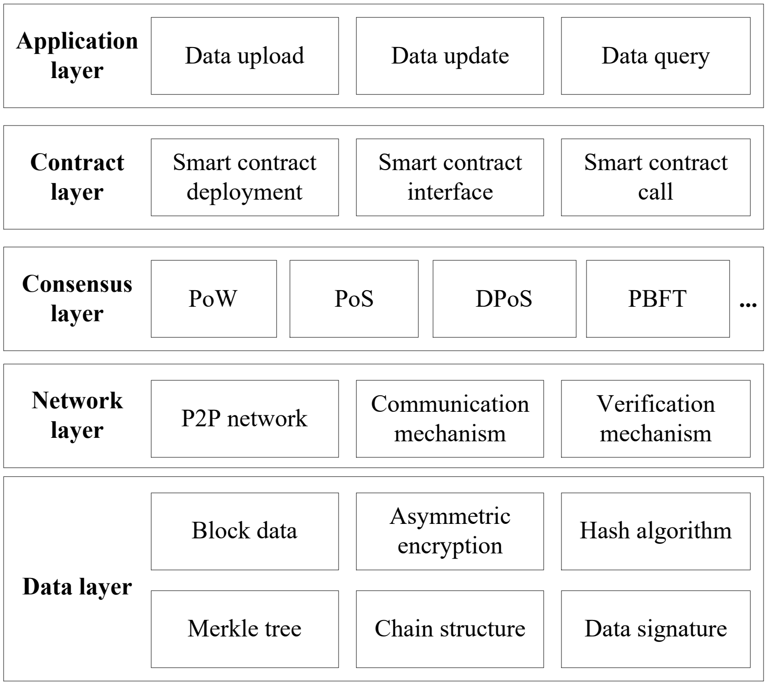

Fig. 1 Blockchain system architecture

The application layer mainly provides an interactive interface for users. This layer encapsulates user requests and submits them to the system for processing, and displays the data returned by the system to users, mainly including record upload and record query, such as uploading students' grades.

The contract layer mainly provides contract deployment, interface and contract call. For example, when the operator invokes the student information addition contract, the operation authority will be verified. If it passes the verification, the student information can be added, and the new information will be recorded in the blockchain.

The consensus layer is mainly coordinated through the consensus mechanism, and the consensus algorithm is used to decide how the participating nodes agree on some specific data. For example, it uses the improved Byzantine algorithm as the consensus algorithm, which is based on the network layer. The network nodes generate new blocks through the consensus algorithm, which ensures that the system can efficiently reach a consensus in the blockchain network and ensure the data consistency of each node in the network.

The network layer mainly provides the propagation function of various data. Based on the propagation of the network layer, each node verifies the received records and blocks. For example, when a network node uploads students' scores, the uploaded scores will be broadcast to the network for verification by other nodes.

The data layer is the basic component to realize the blockchain system. It stores the records and block data of the network layer as corresponding records and block structures according to the principle of cryptography, mainly including hash function, digital signature, asymmetric encryption, Merkel tree, block data, chain data, etc. Among, Asymmetric encryption is usually implemented by Elliptic Curve Cryptography (ECC) algorithm, and the process of encryption and decryption of ECC is as follows.

Step1: Sender A first selects an elliptic curve Ec(a, b) and selects a point from the elliptic curve as the base point P.

Step 2: Sender A chooses k as the private key, at the same time, creates the public key K=kG.

Step 3: Sender A transmits Ec(a, b), K, P to Receiver B through the network.

Step 4: After receiving message sent by sender A, Receiver B encodes the point Z on the elliptic curve Ec(a, b) in plaintext to be transmitted and creates a random integer R.

Step 5: Receiver B calculates points C1 and C2, where C1 = Z + rK, C2 = rG.

Step 6: user B transmits C1 and C2 to user A.

Step 7: After receiving the message, Sender A calculates C1-kC2, that is, C1-kC2=Z+rK-k(rG)=Z+rK-r(kG)=Z.

Step 8: Decode M to obtain plaintext.

### *B. Main process design*

The main process of students' information sharing system includes data upload, data access authorization process, and the data upload process is shown as Fig. 2.

.

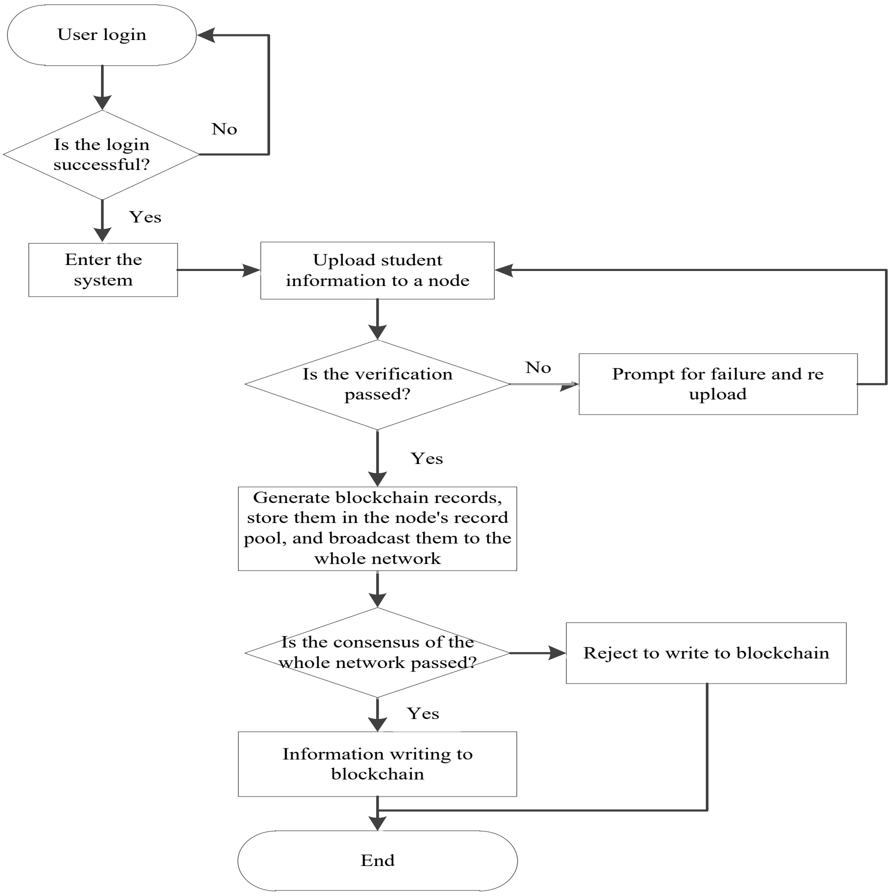
User login
Is the login successful?
No
Yes
Enter the system
Upload student information to a node
Is the verification passed?
No
Prompt for failure and re upload
Yes
Generate blockchain records, store them in the node's record pool, and broadcast them to the whole network
Is the consensus of the whole network passed?
Reject to write to blockchain
Yes
Information writing to blockchain
End

Fig. 2 the Data upload process

(1) Relevant personnel in the school upload the score or education data to their corresponding nodes in the school.

(2) The node receives the data and checks the data. The check contents mainly include the rationality of the data and the signature of the corresponding teacher on the data. After checking that there is no error, the record is resigned, stored in its own record pool and broadcast to the school network; If there is an error in the check, the error result will be returned to the user who uploaded the information and notified to upload it again;

(3) Each node in the school checks the repeatability of the received records, that is, whether the records exist in the local record pool. If not, the received records are subject to a standard record verification process. If the verification is correct, the records are stored in the record pool and broadcast to other nodes. If the verification fails, the records are rejected; If the record exists locally, the record is not forwarded.

(4) A node selects some records in the record pool, packs them into blocks and broadcasts them to the campus network.

(5) The node receiving the block verifies the block. If the verification is correct, wait for a consensus on the block; Otherwise, the block will be rejected.

(6) Each node makes a consensus on the block. If the consensus is successful, the block will be connected to the local blockchain, otherwise the block will be rejected.

Data access authorization is an important means to ensure system security and personal privacy, involving the owner of data, the requester of data and accounting nodes. If the data requester wants to access data, the first operation is login. Only after login verification can he enter the system, and then submit the request for the data he needs to access through the data request module in the system. the data access authorization process is shown as Fig. 3

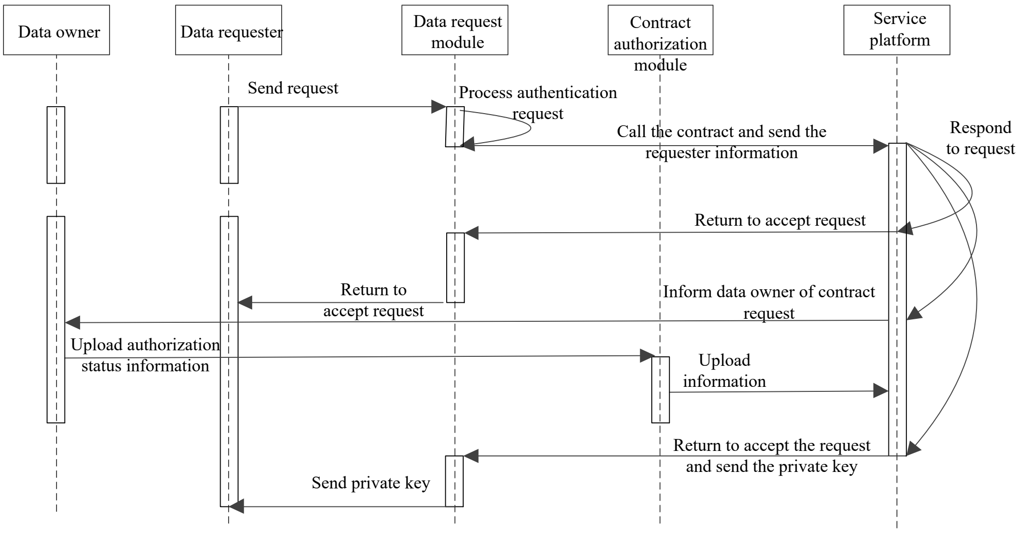
Data owner
Data requester
Data request module
Contract authorization module
Service platform
Send request
Process authentication request
Call the contract and send the requester information
Respond to request
Return to accept request
Return to accept request
Inform data owner of contract request
Upload authorization status information
Upload information
Return to accept the request and send the private key
Send private key

Fig. 3 data access authorization process

## IV. Key Technologies

### A. Consensus algorithm

As the soul of blockchain technology, consensus algorithm has also experienced continuous development and gradually evolved into a consensus algorithm system dominated by PoW, POS, DPoS, PBFT and their related variants. The principles of these four consensus algorithms are briefly analyzed and compared below.

Proof of work (POW) is a consensus algorithm from bitcoin. The understanding of image can be seen as that it sets a puzzle for each production block, and the person who correctly solves the puzzle first obtains the production block right this time. POW relies on computer computing power resources to solve the puzzle, and sets the difficulty adjustment coefficient for the puzzle. Finally, with the support of layers of computing power, the longer the blockchain using POW consensus algorithm, the more reliable and tamper able its historical data will be. Only when the computing power of the perpetrator exceeds half of the computing power of the whole network can the attack be successful. For such an attack, the perpetrator needs to spend a lot of computing power and money resources, which is hard to please. More and more computing power ensures the security of the blockchain, but it also increases energy consumption, which has been criticized by bitcoin. Another problem with pow is that the transaction efficiency is low and cannot meet the system requirements in the actual specific scenario.

In order to solve the problem of high energy consumption and low efficiency of pow, POS is proposed. POS continues the puzzle design of pow, but additionally designs the concept of currency age. The longer the node holds currency, the older the currency age. In order to prevent the node from storing currency indefinitely, the currency age has a time limit. Finally, depending on the number and age of coins held by the node, it is less difficult for the node to obtain the corresponding block right when solving the puzzle, that is, it has a higher probability to obtain the block right. When a node obtains a production block right, the currency age of its spent currency will return to zero, but it will also get the corresponding reward for clearing the currency age. POS is more efficient than POW and solves the problem of energy consumption of pow to a certain extent. However, the design of its mechanism is more likely to lead to node monetization, that is, monopoly, which makes the right to be too concentrated and the user's participation is reduced.

Secondly, POS is more vulnerable to attack without strong computing power and low access threshold.

In order to solve the POS problem, a new consensus algorithm DPOS is proposed. It continues the shareholding mechanism of POS, but the difference is that the algorithm divides nodes into accounting nodes and ordinary nodes. A common node selects a certain number of bookkeeping nodes according to its own shares and the corresponding number of votes. Then, the bookkeeping node selected by the ticket produces blocks in turn. When a billing node fails or generates malicious behavior, the billing node will be stripped of its initial fast rights, and DPOS will vote regularly to select the billing node. DPOS is a low-energy and efficient formula algorithm, but it brings serious centralization problems.

### *B. Smart contract deployment*

After a contract code is finalized, the contract can enter the formal deployment stage. A complete contract deployment process is as follows.

Step 1: One of the participants of the sub chain fills the block with the prepared smart contract, constructs the creation block of the sub chain, generates a sub chain registration record and sends it to the main chain node;

Step 2: The master chain node verifies the sub chain registration record, including verifying each field in the sub chain registration record; After the verification is successful, the master chain node stores the child chain registration record in the record pool, and finally packs the child chain;

Step 3: After the sub chain is registered and recorded in the main chain, the sub chain is created successfully. The main chain block connected by the sub chain is the main chain block containing the sub chain registration record. At this time, the sub chain participant, that is, the participant of the smart contract on the sub chain, can call the smart contract for relevant operations;

Step 4: When the contract is called, the node calling the contract runs the contract in the contract running environment, and a contract call record will be generated at the same time. The contract call record is propagated between the sub chain nodes and finally packaged into the blocks of the sub chain.

Step 5: All sub chain nodes jointly maintain the sub chain in which they participate. When the task of the contract is completed and needs to be terminated, all sub chain nodes jointly sign the contract termination statement, and a sub chain node generates a contract termination record and sends it to the main chain node.

Step 6: The master chain node verifies the sub chain termination record. After passing the verification, the termination record is stored in the local record pool and broadcast in the master chain network. The contract termination record will eventually be packaged on a master chain block. At this time, the whole life cycle of the contract ends.

## V. CONCLUSION

This paper proposes a university student information sharing system based on blockchain technology. The system integrates blockchain technology into university student information management, which not only improves the informatization level of student information management, but also ensures the authenticity, traceability and security of student information, improves the utilization value of student information, and provides reference value for employers to select talents. At the same time, in the management process, the way of multi participation and multi maintenance is adopted to reduce the work pressure of the management department.

## ACKNOWLEDGMENT

This research was supported by Major Project of Philosophy and Social Science Research, Ministry of Education of China under Grant No.19JZD010 and Program of Shanghai Higher Education Society under Grant No. Y1-24.

## REFERENCES

[1] L. Zhi, A.V. Barenji, and G.Q. Huang, “Toward a blockchain cloud manufacturing system as a peer-to-peer distributed network platform,” Robotics and Computer-Integrated Manufacturing, vol. 54, pp.133-144, 2018.

[2] M. Risius, and S. Kai, “A Blockchain Research Framework,” Business & Information Systems Engineering, vol. 59, issue 6, pp. 385-409, 2017.

[3] A.F. Hussein, N. Arunkumar, R.G. Gustavo, et al., “A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform,” Cognitive Systems Research, vol. 52, pp. 1-11, 2018.

[4] Y.H. Dai, G.W. Li, and B. Xu, “Study on learning resource authentication in MOOCs based on blockchain,” International journal of Computational Science and Engineering, vol. 18, issue 3, pp. 314–320, 2019.

[5] S. H. Jeong, and B. Ahn. “Implementation of real estate contract system using zero knowledge proof algorithm based blockchain,” The Journal of Supercomputing, vol. 77, pp.11881–11893, 2021.

[6] C. Sillaber, and B. Waltl, “Life Cycle of Smart Contracts in Blockchain Ecosystems,” Datenschutz und Datensicherheit - DuD, vol. 41, issue 8, pp. 497-500, 2017.

[7] Q.T. Thai, J.C. Yim, and T.W. Yoo, et al., “Hierarchical Byzantine fault-tolerance protocol for permissioned blockchain systems,” The Journal of Supercomputing, vol. 75, issue 11, pp. 7337-7365, 2019.

[8] M. Ren, H.B. Tang, X.M. Si, et al., “Survey of Applications Based on Blockchain in Government Department,” Computer Science, vol. 45, issue 2, pp.1-7, 2018.

[9] K. Fanning, and D.P. Centers, “Blockchain and Its Coming Impact on Financial Services,” Journal of Corporate Accounting & Finance, vol. 27, issue 5, pp.53-57, 2016.

[10] C. Balis, I. Tagopoulos, and K. Dimola, “Moving Towards a Blockchain-Based Healthcare Information System,” Studies in health technology and informatics, vol. 262, pp. 168-171, 2019.