Construction of College Student Credit Information System Based on Blockchain Technology

Liu Xidong[1,a], Shang Yuxin[2], Song Chuanling[3]

Shandong Institute of Commerce and Technology[1,2,3] Jinan, China

[a]20010479@sict.edu.cn

Abstract—In recent years, falsification of learning experience, academic fraud and other academic misconduct are common among college students. However, the data collection and query functions of various management systems used in domestic colleges and universities are relatively single, which is not enough to meet the needs of the society. With the application of blockchain technology in all walks of life, the decentralization, security, credibility and traceability of blockchain technology are highly matched with the construction of College Students' integrity system. The research and development of College Students' credit information system based on blockchain can effectively improve the credibility of the education system, and play a powerful role in promoting the application of education big data and innovation breakthrough.

1. INTRODUCTION to BLOCKCHAIN TECHNOLOGY

In recent years, with the continuous development of blockchain technology and the ensuing digital currency boom, it has attracted widespread attention from various sectors such as industry, government and education. All walks of life have carried out extensive and beneficial exploration and practice around blockchain technology research, such as industrial application and policy supervision.

Blockchain technology is a distributed infrastructure and computing paradigm that uses block chain data structure to verify and store data, uses distributed node consensus algorithm to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses intelligent contract composed of automated script code to program and operate data. This architecture design method can be divided into three levels: protocol layer, extension layer and application layer. The core and bottom technology is in the protocol layer, mainly including network programming, distributed algorithm, encryption and signature, data storage technology. The extension layer is mainly for the implementation of expansion in a certain direction. For example, "smart contract" is a typical application development at the extension level, which is an important development direction of blockchain technology. In the future, with the improvement of the underlying protocol, any product requiring third-party payment can easily use blockchain technology; any information that needs to be confirmed, credit and traced can be realized with the help of blockchain. Application layer is directly oriented to users, similar to various software programs in the computer.[1]

2. FEASIBILITY ANALYSIS OF USING BLOCKCHAIN TECHNOLOGY TO CONSTRUCT COLLEGE STUDENTS' CREDIT SYSTEM

In recent years, academic misconducts such as forging learning experiences, plagiarizing academic research results of others, and tampering with personal scores are common among college students. However, the current credit information system used by domestic colleges and universities is relatively

simple in data collection and unable to objectively evaluate the quality of talents. Take the China Higher Education Student Information Network ("Xuexin.com" for short) as an example. It only provides basic information such as certificate of student status, registration of new students, school attending or graduation. In addition to paper files in universities, there is no easy-to-find historical data information chain, which makes it impossible for governments and employers to obtain complete and effective information. So schools and various educational institutions are required to provide query services for students in real-time verification.

2.1. Business Requirements Analysis

From the perspective of business needs, college students' credit information system needs to record the growth process of students from enrollment to graduation and employment, at least including basic modules such as student status information, performance information, reward and punishment information. It is a system with continuous data updating over time, and in addition to some public information, there are some that are only specific to the system The system needs to provide different access control for different users. All registration information must ensure the authenticity and existence, and can trace the entire process of student growth. In short, the design goal of the college student credit system is to build a decentralized system that not only guarantees the disclosure of some information, but also prevents malicious tampering. All registration information must ensure the authenticity and existence, and can trace the entire process of student growth. In short, the design goal of the college student credit system is to build a decentralized system that not only guarantees the disclosure of some information, but also prevents malicious tampering.

2.2. Analysis of the fit between system requirements and blockchain technology

First of all, if the traditional centralized data system is adopted, a large amount of data will be generated in the system in the long-term use process. These data are stored in the central database (one database plus multiple copies), which makes the management of the server very difficult. Moreover, the database administrator or system administrator can directly modify and delete the data from the background, The security and credibility of data cannot be guaranteed. Secondly, students can not directly view personal credit information, only through school information certificate issued by the school, the school's file management is a great challenge. Thirdly, it is very difficult for employers to verify the information of students. In this way, even if students falsify their resumes and academic qualifications, enterprises can not verify it.

Blockchain is a network and database technology architecture to solve the credit problem. Through the consensus mechanism of distributed nodes, the trust between unfamiliar nodes is established, and through the common maintenance of the whole network, the authenticity, reliability and immutability of massive transactions are guaranteed. The value of blockchain is that it can establish trust in the case of asymmetric information, without the supervision and approval of the central management organization, which greatly improves the transaction efficiency and reduces the transaction cost.

- Compared with the centralized system, it not only has transparent information, but also avoids the network load of the central database.

- The data in the blockchain is jointly managed by all nodes that join the blockchain network, and the stored data will not be modified by a single node. The transaction data of the blockchain is completely stored in each computer node, recording the input and output of each account, so as to trace the information changes and bookkeeping activities of each user, and make all accounting information transparent and searchable.

- The system can ensure the security of stored information, solve the problems of information loss and tampering, and forge identity information.

From the above analysis, blockchain technology has natural advantages in college students' credit information system. Research and development of College Students' credit information system based on

blockchain can effectively improve the credibility of education system and reduce the workload of schools, enterprises and institutions.

3. TECHNICAL SCHEME OF COLLEGE STUDENTS' CREDIT INFORMATION SYSTEM BASED ON BLOCKCHAIN

The ultimate goal of College Students' credit information system is to ensure the safety, credibility and traceability of data, so that the information provided by the system can be reliably shared among students, schools, enterprises and institutions.[2] The system can provide students' status information, academic performance, vocational qualification certificate, skills competition award-winning, social practice and other data, which can be used for employers to check students' status information and ability, and can also be used for tracking research of graduates in Colleges and universities. The system involves thousands of teachers and students in colleges and universities. In addition to preventing the risk of fraudulent resumes, the traceable credit data also provides the possibility of precise screening of corporate human resources and personalized services.

3.1. Ethereum smart contract

Smart contract is a set of promises defined in digital form. If a contract is operated under the condition of unchangeable and public supervision, the party who violates the contract will pay a predetermined price. This system selects Ethereum, which is the most common development contract, and is developed by solidity language and runs on Ethereum virtual machine (EVM). When running in EVM, each step of operation is executed by all nodes at the same time, which ensures the consistency of smart contract at the same time.

The smart contract of Ethereum is driven by event. Multiple users work together to formulate a corresponding criterion. After all users reach an agreement, the contract state is stored on the blockchain. When the event occurs, the contract state is updated to judge the state machine. The business logic it writes provides services and interfaces for its front-end application development. If the corresponding conditions are met, the state machine automatically executes the smart contract code according to the preset response rules, the contract execution results are output to the user, and the contract value and state changes are recorded on the blockchain.

3.2. DPOS consensus mechanism based on grouping

College student credit information system involves many student users and enterprise users. If all users become the blockchain consensus participants of the system, the network maintenance cost of the system will be greatly increased, which will bring great challenges to the implementation of specific software and hardware. Therefore, according to the characteristics of different roles of users involved in the credit system of college students, selecting the nodes trusted by the users of the credit information system to generate each individual information block is the basic principle that the consensus of college students credit information system based on blockchain can reach.

DPOS consensus mechanism is to select proxy nodes by voting among a large number of nodes, and generate blocks by proxy nodes, so as to achieve rapid consensus verification, greatly improve the throughput of the system, and meet the needs of College Students' credit information system based on blockchain, which is the preferred way of consensus mechanism. The core idea is to determine the number of accounting nodes M in advance. All nodes in the whole network can decide which nodes can become bookkeeping nodes(witness) by election. The nodes with the top M votes have the right to be selected to create blocks. Because of the limitation of the number of accounting nodes, we can specify a relatively short block time in the consensus algorithm, and make bookkeeping by taking turns.[3]

According to the system requirements, this paper uses the consensus framework based on grouping to divide all user nodes into four groups: University node set, student node set, enterprise and institution node set, and education authority node set. [4] According to the system requirements, this paper uses the consensus framework based on grouping to divide all user nodes into four groups: University node set, student node set, enterprise and institution node set, and education authority node set. Each group

conducts election and voting, and selects a certain number of proxy nodes to exercise the proxy power of the node set. The four groups of selected proxy nodes form a proxy node set to produce blocks and verify blocks.
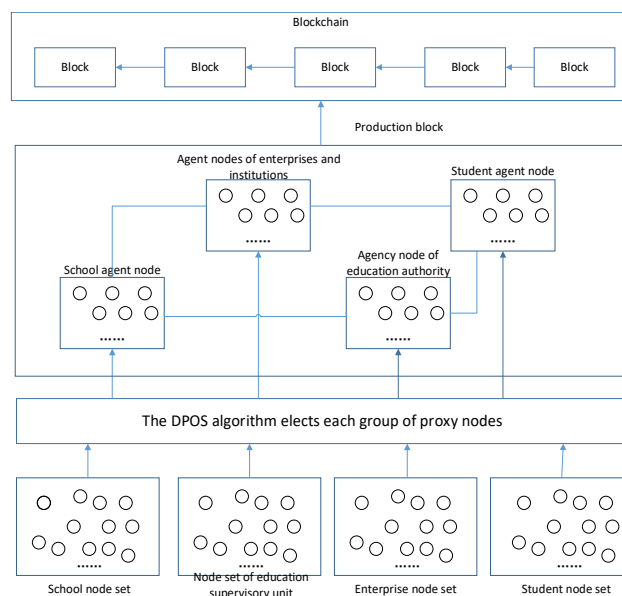

Figure 1.   DPOS consensus mechanism based on grouping

In the constructed blockchain, the educational authority is the regulatory agency of the blockchain system, which uniformly formulates the operating standards and contract conditions of the blockchain. Each node and participant on the blockchain must follow the pre-established transactions Rules participate and run. All node related operations need to be authenticated by consensus mechanism. According to functions, it can be divided into three categories: client nodes, proxy nodes, and voting nodes. According to different roles, client nodes are divided into four categories: students, universities, enterprises and institutions, and education authorities. The university node restricts and manages the permissions of various users through smart contracts, is responsible for adding, deleting, checking and modifying the students' academic performance, professional ability, and professionalism, and is responsible for the authenticity and validity of the ledger. The student node contains the basic information of each college student, colleges attended, rewards and punishment information, major events, etc, representing the digital identity of each individual college student in the alliance chain, and can query and verify information. Enterprises and institutions can track the learning behaviors of students during school, and use the trusted data analysis of the internal nodes of the alliance chain to determine whether they meet the development needs of the company. Each node on the block chain operates on its own according to a pre-appointed algorithm, thus forming a distributed credit management system that cannot be tampered with, traced back, and can be queried.

3.3. The system architecture of the college student credit information system based on blockchain
The design and implementation of this system is based on the truffle framework provided by Ethereum, and the alliance chain is selected, which involves front-end development, smart contract development, and Ethereum interface calls. The entire blockchain system is composed of multiple isomorphic complete data nodes that are mutually backed up by voting to generate proxy nodes, new blocks are generated through proxy nodes, and each block is stored after an agreement is reached. At the same time, when choosing a consortium chain, only authorized nodes can join the network, and information can be viewed according to permissions. The nodes are highly credible, so the transaction process does not need to be verified by every node. Therefore, the transaction speed is faster and the transaction cost is lower.

The system structure of the college student credit information system based on the alliance chain is as follows:
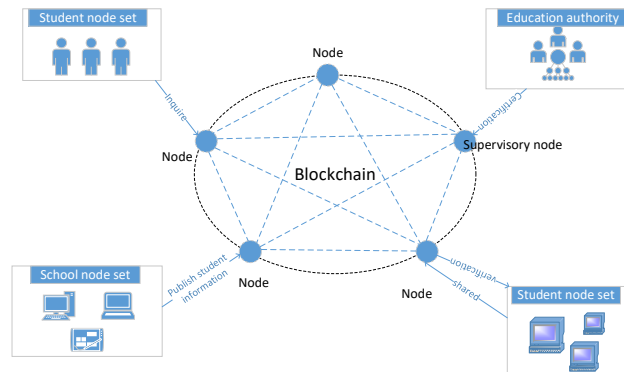

Figure 2.   the system structure of the college student credit information system

The system is mainly divided into three layers, from top to bottom are user layer, extension layer and protocol layer, as shown in the figure 3.

The user layer mainly includes front-end user interface (UI) and system function modules. The front-end UI mainly provides a visual web interface for users to access the college student credit system, mainly using html/Bootstrap language. The system functions realize the foreground display of background data and different business operations of different users, such as system management, user login, adding information and querying information. The front-end application also realizes the interaction with the smart contract. All successful operations will form a new block after node verification, and then broadcast all business nodes to update the block information to ensure the integrity and consistency of all business nodes.
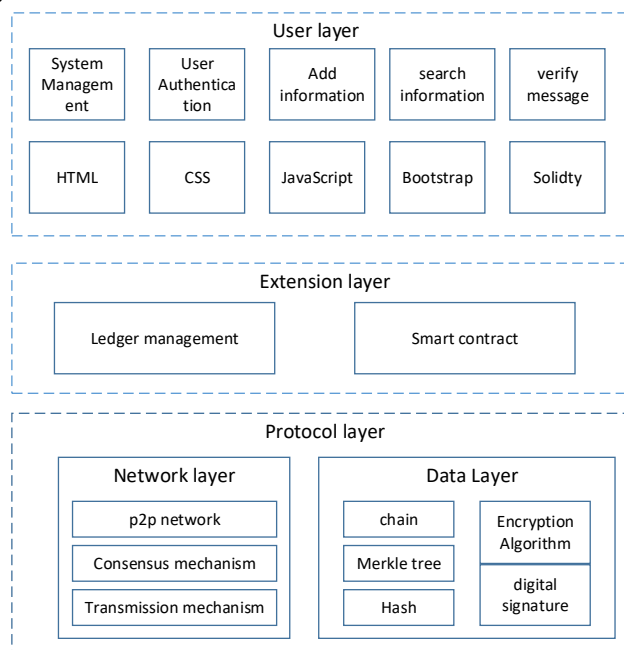

Figure 3.   Blockchain-based college student credit system architecture

The expansion layer is mainly ledger management and smart contracts. [4] Ledger management is based on certain consensus rules, and uses multi-party decision-making and joint maintenance methods

to store and copy data to ensure that the source of information is unique and true and reliable, thereby ensuring the traceability and traceability of student data. Smart contracts can be automatically executed under certain conditions. Business processes such as uploading, deleting, querying, sharing, and verifying are all realized through smart contracts. The business logic it writes provides services and interfaces for its front-end application development. For example, in the information verification process, the smart contract interface is called to calculate the hash value of the uploaded data, and the hash value in the block is verified. Smart contracts enable us to execute safe, reliable, traceable and irreversible transactions without the participation of third-party institutions.

The protocol layer mainly includes the network layer and the data layer. The network layer is responsible for information communication, consensus generates new blocks, and maintains the stable operation of the blockchain network. The data layer is the decentralized database of the system, which stores the data information generated by system node transactions. The system uses encryption algorithms such as RSA and AES, digital envelopes and digital signatures to ensure the legitimacy of the credit information system for college students.

The specific business process is as follows:

3.3.1. Initialization. After the school node is initialized, the authentication registration is performed on the smart contract, and the school's transaction address is stored in the smart contract.

3.3.2. Production block. The school enters and publishes student node information, and passes the student signature, school signature, number and other information into the smart contract. After the proxy node reaches an agreement through the DPOS consensus algorithm, the information is confirmed to be valid, and the proxy node that generates the block generates a new The block is broadcast to the whole network.

3.3.3. Verification. After receiving the new block, the nodes of the entire network verify whether the new block is correct and trustworthy. If most nodes in the network reach a consensus on the new block, the block will be added to the blockchain.

3.3.4. On the chain. The agent node adds the new block to the blockchain to form the latest complete chain.

4. CONCLUSION

With the rapid development of my country's economic construction, the construction of the integrity system of the whole society is seriously lagging behind, especially the lack of integrity of college students has attracted widespread attention from the whole society. [5] With the help of technical means such as blockchain, the integrity of the education system is improved and schools are established. The credible data sharing mechanism with society is of great significance to the emergence of new educational models.

REFERENCES

[1] Do you really understand the six tier architecture of blockchain?
   https://www.jianshu.com/p/5e72bb776280.
[2] Wu Kunxiong, On the design principle of commodity trading platform based on blockchain, Fujian Computer 2018, No. 11, pp.125-126
[3] Zhou Ruyue, Qian Liang. Distributed Digital Rights Management Mechanism Based on Blockchain Credit System, Computer Application Research.
   https://doi.org/10.19734/j.issn.1001-3695.2018.11.0870
[4] Hu Yafei, Research on blockchain consensus mechanism for school educational administration system .

https://xueshu.baidu.com/usercenter/paper/show?paperid=1w0t0eh0xp6a0jd0tv2f0v70pq534 237&site=xueshu_se

[5] Zhang Xiaoli, Design and implementation of College Students' credit reference system based on blockchain. Journal of Zhejiang Sci-Tech University(Social Sciences),Vol.40,No.6,Dec.2018.