Design of Student Capability Evaluation System Merging Blockchain Technology

Wenshuang Zhao¹, Kun Liu²*, and Kun Ma³
¹,²School of Information Science and Engineering, University of Jinan Jinan 250022, PR China Nanxinzhuang Road No. 336
* Corresponding author: liukun@ujn.edu.cn

Abstract. This article mainly introduces the application program of blockchain technology in the evaluation of students' professional ability. Through K-means clustering algorithm, students' academic performance and academic achievements in school, training, competitions, practice and other activities outside school are analyzed, in order to objectively and effectively evaluate the students' professional ability, which provides reasonable advice for student employment. In the system design, the blockchain technology is applied to the student ability evaluation system. The blockchain technology provides distributed storage and is non-destructive and traceability, so as to achieve the overall monitoring of students' professional ability evaluation process, student assessment data can be traced and student learning credit can be increased anytime anywhere. This paper presents a design scheme of the student ability evaluation system based on blockchain technology, which includes a student ability analysis method based on clustering algorithm and an overall system architecture diagram based on blockchain technology, which provides possibilities for creating an ecosystem of student ability evaluation for the future.

1. Introduction
At present, the student capability evaluation system has been perfected in data acquisition, evaluation schemes and indicators, and the most commonly used evaluation methods are quantitative and qualitative, including AHP, BP neural network, data mining and SSPS linear regression analysis [1] [2]. However, there are still defects in system information security and credibility. Firstly, in terms of system information security, traditional developed systems are easy to be attacked, and students' professional ability assessment needs accurate data and information. For example, maliciously tampering with students' grades or test questions lead to the deviation of the evaluation results and affect the students' training direction. Secondly, in terms of credibility, the result of the student capability evaluation system is a proof of all the performance of a student during the school period. When a student is looking for a job or continuing his studies, the system can serve as the most convincing reference for the admission party. Thirdly, data traceability, if there is any doubt about the result of students' capability evaluation, the evaluation process of students can be traced back.

Blockchain technology can solve these problems. The concept of blockchain was appeared in a post by Satoshi Nakamoto on bitcoin BBS for the first time in late 2008 [3]. Blockchain is a decentralized distributed data management technology through data encryption, data chain hook, multi-copy storage and distributed consensus. Blockchain is a decentralized distributed database, which protects information security and authenticity [4]. Each block contains the hash value of the
previous block and ensures the traceability of data on the chain. Therefore, blockchain can provide strong technical support for the security and credibility of the student capability evaluation system.

In this paper, we describe the system design scheme based on blockchain technology, including the evaluation method and the system architecture model.

2. Introduction to Blockchain Technology

2.1. Structure of Blockchain

The unit of blockchain is the block, while the block is a data structure that used to record transactions. Each block consists of block body and block header. Where, the block body only records all of the transaction information for a period of time before. The structure of the block header information is shown in Fig.1. One of the most important information contained in the block header is the hash value of the previous block, this is the key to connecting all the blocks, and the main reason why the block chain is hard to tamper and can't be forged, and can be traced back.

![Figure 1. Structure Diagram of Block](image)

Parent hash value: the hash value of the previous block.
Merkler root: used to test whether a transaction exists in the block.
Time stamp: record the time that the block is generated.
Difficulty value: the computing power required to generate the block.
Random number: calculate this number to produce the block.

2.2. Consensus Mechanism

The consensus mechanism is the core of the block chain, which is related to the normal operation of the block chain. The so-called consensus mechanism is the algorithm that all nodes reach consensus on transactions in a period of time[5]. The most commonly used consensus mechanisms are Proof of Work-PoW, POS Proof of Stake, Practical Byzantine Fault Tolerance.

2.3. Characteristics of Blockchain

2.3.1. Decentralization

The blockchain transmits data information through the point-to-point network and jointly maintained by multiple nodes. Each node verifies that the information received by other nodes is correct while it receives information, there is no third parties are involved.

2.3.2. Reliability

Each node on the blockchain contains the same data information, which is equivalent to the backing-up by each node. The system will not be down due to the damage of one node. The system will be paralyzed when the damaged nodes are more than 51%. In addition, there is a direct connection between blocks. Each block contains the hash value of the parent block. It is assumed that to tamper with the data on the blockchain requires a lot of computer power, so blockchain is a very reliable distributed database.

2.3.3. High Trust
Algorithm is the basis of mutual supervision and self-restraint between nodes on the blockchain. When malicious nodes attack the system, other nodes will stop it effectively. And every transaction is completely transparent on the blockchain. The node verifies each transaction through digital signature, reducing the trust risk of the system effectively.

2.4. Type of Blockchain
There are three types of blockchain: public chain, private chain and alliance chain.

| Type                | Characteristic                        | Application scenes                      |
|---------------------|---------------------------------------|-----------------------------------------|
| Public blockchain   | Less access barrier, open data        | Bitcoin, Ethereum                       |
| Private blockchain  | Privacy protection, low transaction cost | Private institutions with the single-center network |
| Alliance blockchain | Low operation and maintenance cost high transaction speed, | B2B transaction between different entities |

3. Design Scheme of Traditional Student Capability Evaluation System

3.1. Student Capability Evaluation System
Student capability evaluation system is a dynamic evaluation platform for college students' ability, which realizes the dynamic evaluation on students' ability through long time data collection. Firstly, data collection is carried out, where the content of data collection includes students' academic performance, systematic answer scores, academic achievements and off-campus practices. Then it enters the evaluation stage and realizes the student capability evaluation in the form of data mining. Finally, the ability level of the most representative students in the group is determined as the evaluation standard through clustering, and the similarity degree with students to be evaluated is compared to determine the ability level of the students to be evaluated. Figure 2 is the specific process of student capability evaluation.
3.2. Analysis of Key Problems

The student capability evaluation standard is a key problem in the system development process, and our research group has adopted SimRank algorithm to solve this problem. SimRank is a model based on graph topology information to measure the similarity between any two objects, which was first proposed by professors Glen Jeh and Jennifer Widom of MIT laboratory in 2002\(^6\). In order to achieve better experimental results, members of our research group have improved the original SimRank algorithm. The improved SimRank algorithm formula is as follows:

\[
S(a,b) = \frac{1}{|V(a)||V(b)|} \left( \sum_{i \in V(a)} \sum_{j \in V(b)} \delta(i,j) S(i,j) \right)\]

(1)

The scheme was verified by the collected information, and the verification results are as follows:

---

Figure 2. Specific Process of Student Capability Evaluation

Figure 3. Distribution of Students' Two Professional Abilities

Figure 4. Correctness Verification of Ability Evaluation Standard
4. Design Scheme of Student Capability Evaluation System based on Blockchain

As the core support of the bitcoin system, the blockchain technology has the characteristics of decentralization, trustlessness, transaction transparency and tamper-resistance. According to the structural characteristics of the blockchain, the "transaction" in the student ability assessment system, that is, the operation related to the student ability evaluation, will be broadcast to every node in the network to ensure that the operation process of the student ability evaluation result is open and transparent, and can not be tampered with.

In order to ensure monitoring of students' professional ability evaluation process proverbially, the "source" should be credible in the first place. Therefore, the system to authenticate students needs to limit the scope of the IP. On the other hand, the reference value of student capability evaluation not only depends on school course grade, but also includes academic achievements and off-campus practice. The content of student capability evaluation is uploaded to the blockchain as a "transaction" to enable students, so as to increase their learning credit at any time and any place. Since all the blocks on the blockchain are interconnected, the data stored can be traced.

4.1. System Design

The system is divided into application interaction layer and blockchain layer. The interaction layer belongs to the upper layer of the system. The blockchain layer is the bottom layer of the system, as shown in Fig.3:

```
Figure.5. Architecture Diagram of Student Capability Evaluation System based on Blockchain Technology
```

The upper interaction layer that can directly interact with users, thus receive and feedback information by user operations, in addition, it is responsible for encapsulating user data, that is, information related to student capability evaluation results, into "transactions" submitted to each node and then transmitted to the blockchain.

The blockchain layer includes P2P network nodes and underlying blockchain. P2P network nodes are used for receiving encapsulated "transactions" from the interaction layer, and verifying the "transactions", finally all of nodes will be voting for new blocks. Blockchain is used to store all "transactions", that is student capability evaluation results.

4.2. P2P Network Nodes
Data in blockchain is spread in a P2P network\textsuperscript{[7]}. In order to enhance the credibility of the student capability evaluation system, the node setting includes each college in university and relevant education departments. All of Universities and supervision education departments can check the information released by the system at any time, and enhance the credibility of the student capability evaluation system while improving the talent training competitiveness of each university.

4.3. Authentication

In the student capability evaluation system based on blockchain, the dual database technology is adopted. The system operation data is stored in the general relational database and the information of students’ capability evaluation results is stored on the blockchain. The public key and private key are needed on the blockchain as the authentication condition for receiving and sending "transactions".

In this system, all participants will get a pair of secret keys. The private key is the identity certificate of the individual or unit. When writing the transaction, the private key is written on the transaction as a digital signature to confirm identity of the transaction sender. The public key is equivalent to an account. When sending a transaction to another node, the receiving address writes the public key of the recipient, who must use his own public key to unlock the transaction. Each student has a public key, and students' grades and professional competence level can be inquired through the public key. If the public key can be used to query students' information, that indicates that the student's ability evaluation result has been successfully stored on the blockchain.

4.4. Transaction Process

The information conveyed in the student capability evaluation system is encapsulated into a virtual asset for "transaction", and students, teachers, schools and education bureau are all "traders". Students create virtual assets, such as student's name, number and major, the above information is encapsulated into "trade", generate a digital signature with the private key, and send the transaction to the teacher. The account of transaction receiver is the teacher's public key that is used to unlock received transaction. Three core fields of student name, student number and major are extracted after verifying the identity of the student. The name, number, major, course result, academic achievement and practical experience of the student are created and sent to the school as the transaction. The school receives the transaction from the teacher, and unlocks it with its own public key. After the student capability evaluation, the school will present the student's name, number, major and capability evaluation results as the transaction to education regulatory authorities. Therefore, in this system, the education department is not only the node in the network, but also the subject of transaction. In order to facilitate data entry and sharing, all transaction data on the blockchain is saved in JSON format.

4.5. Creating Blockchain

Before block generation, at first, the node that receives the transaction verifies whether the transaction is legal. After the verification, the transaction is put into the new block. The hash value of the new block is calculated by the node, and the hash value is unique on each block. And then the node airing the new block to other nodes, and other nodes start to vote, which is to confirm whether the transaction on the block is legal. If the new block is approved, it will be added to the chain. As the number of legal transactions increases, the size of the blockchain will be larger and larger.

The above is the overall design of the student capability evaluation system based on blockchain technology and the main process of storing data to blockchain.

5. Conclusion and Prospect

In this paper, a design scheme of student capability evaluation system based on blockchain technology is proposed, and a secure and notarized student capability evaluation platform is built based on the traditional student capability evaluation system. This paper introduces the blockchain technology, including its structure, consensus mechanism, characteristics and type, and then introduces the traditional student capability evaluation system, detailing the key problem in the
process of system development and solving the problem of SimRank algorithm. The final part is the overall design idea of the student capability evaluation system applying blockchain technology, including system architecture diagram, network node construction and related processes of student capability evaluation results stored on blockchain.

At present, the popularity of blockchain technology is increasing, and the application field is gradually increasing as well. However, the blockchain technology still needs further research and exploration in the field of education, and we are looking forward to the new breakthrough of blockchain technology in the field of education.

References
[1] Liu T. The Application of AHP on the Evaluation of the Student's Comprehensive Quality[J]. Value Engineering, 2011.
[2] Wang N, Huang G, Lei W U, et al. Research on physical fitness assessment of undergraduates based on artificial neural network model[J]. Journal of Nanchang University, 2016.
[3] Beck R. Beyond Bitcoin: The Rise of Blockchain World[J]. Computer, 2018, 51(2):54-58.
[4] Peck M E, Moore S K. The blossoming of the blockchain[J]. IEEE Spectrum, 2017, 54(10):24-25.
[5] Eyal I. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities[J]. Computer, 2017, 50(9):38-49.
[6] Zheng W, Zou L, Feng Y, et al. Efficient simrank-based similarity join over large graphs[J]. Proceedings of the Vldb Endowment, 2013, 6(7):493-504.
[7] Ametrano F M. Bitcoin, Blockchain, and Distributed Ledger Technology[J]. Social Science Electronic Publishing, 2016.