Student Performance Protection Based On Blockchain Technology

Xiao Liang¹, Shiyuan Xu²*

¹ Data Science and Technology, North China University of Technology, Beijing, Beijing 100144, China
² Information security, North China University of Technology, Beijing, Beijing 100144, China
*Corresponding author’s e-mail: 18151010714@mail.ncut.edu.cn

Abstract. In recent years, performance management has become more and more significant in terms of management and credibility of universities. They have to review student performance when issuing diplomas. Therefore, the reliability of student performance management is extremely important. Nowadays, many universities adopt a data-centralized management model. However, centralized database often brings about problems such as information leakage and easy tampering. With the development of blockchain technology, its decentralized and unforgeability characteristics have gradually attracted people's attention. In order to prevent students' scores from being maliciously tampered with, we utilize blockchain to design and implement a decentralized student score sharing management system. Moreover, by using the Ethereum smart contract to manage on-chain and off-chain data storage as well as on-chain query and verification, we ensure the traceability, tamper-proof, distributed storage, and the security of query process. Finally, this article explores the construction of prototype system based on the Ethereum environment. The experimental results show that the anti-tampering and traceability scheme proposed in this article is feasible. The application of blockchain can fully satisfy the needs of various participants in student performance management. Each subject's information has a separate decryption private key, which perfectly protects student's score information.

1. Introduction

These years, with the continuous development of IT technology, much more student information is basically stored using digital technology. Many universities and colleges adopt computer information systems to store information such as student grades [1]. Student performance is a crucial criterion for the issuance of graduation certificates as well as employers' reference and the performance management system has been an essential tool to manage performance. However, with the importance of student performance increasing gradually, many adversaries attacked school's score recording system, stealing or destroying school server data, and affecting students’ final graduation scores.

At present, most schools utilize management platform which are based on centralization[2]. Although the information processing process is simplified and the student performance management becomes more efficient, it is also accompanied by potential security risks. For example, the risk of a single point of failure: once the central server has a problem, the entire system will stop running, which may cause damage to the data stored in the system; the risk of a single point of breach: if the administrator account of the management server is attacked, then the attacker could modify student
scores without being noticed. In addition, the administrator himself can also modify student scores maliciously, destroying the authenticity and integrity of the data.

In response to the security issues mentioned above, this article describes the use of blockchain technology in the traditional student performance management system to store and query student data on and off the chain, so as to overcome the above shortcomings and improve the reliability of the student performance management system. The specific ideas of this article are as follows:

① We utilize blockchain in the performance management system, rely on the advantages of blockchain technology, and increase the reliability and credibility of the system through cryptography in an environment where multiple parties are not need to trust each other. The Ethereum platform establishes a distributed multi-ledger, stores the score information in blocks, and passes the encryption verification of the link between the front and back blocks, ensuring that the information cannot be tampered with and can be traced.

② We adopt the Keccak-256 algorithm of Ethereum and the K-anonymity methodology of blockchain to prevent information leakage and ensure privacy and security effectively.

③ Our system is based on the characteristics of equal rights and co-construction of blockchain technology and optimize index information in order to realize fast retrieval function.

2. Related Work
At present, most of the performance management systems adopt B/S architecture so as to the data is stored in a centralized system, which is extremely easy to be attacked. Meanwhile, the database administrator has a higher authority and can add, delete, modify and check the data freely. With the development of cloud computing and blockchain technology, the advantages of B/S architecture are becoming less and less obvious, and it has becoming much less suitable for people's various needs in terms of response speed and security.

Satoshi Nakamoto proposed blockchain technology, which uses a decentralized methodology to greatly improve the security of the system. Since the birth of Ethereum, scholars and researchers have conducted a lot of researches and discussion on blockchain applications [3,4]. Then, Galal[5] proposed some possible solutions to the security and privacy issues of the Internet of Things(IOT) based on blockchain and Ethereum. Afterwards, Claudia Pop[6] designed a distributed ledger based on blockchain to prevent tampering and the prototype verification is implemented on the Ethereum platform. Researchers proposed multiple smart contract templates based on the Ethereum platform, which are well applied to various fields [7]. Blockchain technology has attracted the attention of many scholars in the fields of finance, IOT, energy, etc. Meanwhile, the data encryption, anti-tampering and traceability characteristics of its prototype system have been verified through the Ethereum platform. Its application prospects are broad and it has great promotion value.

3. Current Systems and Threat Model
We reviewed current system models and proposed some threat models. To begin with, we inspected current system model with blockchain and found that when these systems need to modify student scores, they usually have to submit an application before they can be changed. This method has the hidden danger of data tampering, and malicious attackers can capture the application. Furthermore, having revised the application and analysed the datagram to capture private information, it could lead to some potential privacy threats.

Our system ensures that supervisors and students have only data read-only permissions in terms of identity verification and data changes through using blockchain and smart contracts, thus the ability to resist tampering of our system has been enhanced significantly.

4. System
In this article, we propose a smart contract platform based on Ethereum, building a private chain on access to cloud data, combining score management with blockchain technology to ensure data integrity in the university performance management system.
4.1. System process
Our system is divided into several parts, as input part, query part, and supervisors part. Different subjects have different corresponding interfaces. System flow is shown in Figure 1 below.

In our system, we firstly introduce teacher part. Teachers can log in the platform to enter the student score and fill in the course name, number, and student information. Then, we encrypt the score information and upload it to the information chain through the smart contract. Moreover, they can upload the retrieval information which composed course name and course number to the retrieval chain.

Secondly, we sketch student part. Students can log in to the platform to find their own course score information through the search chain which was saved in the database. When submitting their scores to the employer or the school for further studies, student will get a QR code encrypted with their own public key, which is used to verify their information. Having scanned the QR code, it needs to be confirmed by the student. Last but not least, having decrypted by the student's private key and returned to the score information, they can verify the authenticity of the data in real time, and there are no leakage in the intermediate link, which increases mutual trust.

4.2. System architecture
We establish the score catalog index information as well as score information chain on the blockchain Ethereum platform. The score data will be encrypted and written into the blockchain, and the key will be generated automatically.

The overall architecture of the score information database system is shown in Figure 2. It contains four modules: blockchain module, smart contract module, database module, and client module.
4.3. **blockchain module**

The main function of the blockchain module is to package data which was submitted by users on the chain into blocks, and the participating nodes in the network will connect the blocks to the end block of the chain after being confirmed by the consensus mechanism in order to data storage, traceability query and also ensure the security and integrity of data.

4.3.1. **Authentication.**

In this article, we propose the RSA asymmetric encryption algorithm in the system. The public key is utilized to testify user's identity in the system, and the private key is used for digital signatures, thus ensuring the authenticity of the user's identity.

We use Keccak256 algorithm to protect stored data. The certified score is encrypted with public key, and the demander uses the private key to decrypt and verify the score. As for retrieval method, we utilize the Keccak256 algorithm to form a summary which can encrypt hash, random number, time stamp, and incoming data of the previous block to obtain a 256-bit character as to hash address. The management key is generated through the key derivation tree, and the data key of each sub-chain is derived from the root key. The data between the sub-chains is invisible to each other, and the root key owner can view the data of each sub-chain.

The iterative structure used by the Keccak algorithm is the Sponge structure. And the process of constructing F function from Sponge structure [8] is marked as SPONGE[f, pad, r]

\[ f: b \text{-bit conversion; } b: \text{width, } b=r+c, b>r; \text{ pad: padding rule; } r: \text{ bit rate, the value is 1088bit in keccak256} \]

The Keccak algorithm is marked as Keccak[r, c]:

\[ \text{Keccak}[r, c] = \text{SPONGE}[\text{Keccak} - f[r + c], \text{pad}10 * 1, r] \]  \hspace{1cm} (1)

\( r+c \) is the width of Keccak algorithm compression function Keccak-f_r+c\in\{25,50,100,200,400,800,1600\}

\[ \text{Keccak}[c] \equiv \text{Keccak}[r = 1600 - c, c] \]  \hspace{1cm} (2)

\[ \text{Keccak}[c] \equiv \text{Keccak}[c = 576] \]  \hspace{1cm} (3)

The Keccak algorithm defines four variables with fixed output lengths, \( n=256 \) used in this article.

4.3.2. **Authentication mechanism.**

Whenever the data changes (such as added or maliciously modified), the verification mechanism will be triggered. If is data addition, the mechanism will verify whether the calculated hash is correct, whether the previous block hash is correct, and whether it is the last block. If the data is maliciously
modified, it will recalculate whether the hash is correct, verify whether the previous block hash is correct, and verify whether the previous block hash of the next block is consistent with the current hash.

4.3.3. K-anonymity.
The system described in this article uses the K anonymity algorithm to encrypt and desensitize the stored data. Illegal attackers can only acquire ciphertext. Thus, it is impossible to confirm which certain piece of data corresponds to and cannot be decrypted and identified without owning the secret key.

In order to measure the grade of anonymity, information entropy can be proposed for the privacy group. We suppose every individual in the anonymity model of x as an information point, so we take H(x) to show its entropy value. After that, we assume pi is the possibility to analyse the ith one in the anonymity set with k members.

\[ H(x) = -\sum_{i=1}^{k} p_i \log_2 (p_i) \]  

(4)

\( H_M \) is the maximum entropy where the k-anonymity set is accomplished when all students have the same possibility of 1/k to be spotted. Therefore, we can easily get:

\[ H_M = \log_2 (k) \]  

(5)

Furthermore, the information that adversary can achieve could be totally expressed as:

\[ d = 1 - \frac{H_M - H(x)}{H_M} \]  

(6)

which is standardized and divided by \( H_M \). According to this, the anonymity degree is defined by Diaz et al. As:

\[ d = 1 - \frac{H_M - H(x)}{H_M} \]  

(7)

4.4. Smart contract module.
The student achievement system establishes a private chain on the Ethereum platform, providing access to nodes for relevant personnel, data retrieval and use for all persons in need through permission. The system provides corresponding interactive interfaces to teachers of various subjects. The data submitted by teachers is stored on the chain through smart contracts, and its legality of data is ensured through asymmetric encryption. We write and implement smart contracts based on the Solidity language so that various source data are stored, queried and used on the chain by writing an interactive interface. After the contract is compiled and generated, the corresponding functions in the smart contract are called to complete the protection and storage of data.

4.4.1. On-chain storage query of score information.
Having completed the certification of the authenticity of the score, teachers have to submit the data, using smart contract to encrypt score information and writes it into the block on the chain, and generates the key to complete data on the chain. In our system, we store hash index, private key and teacher’s information in the relational database according to the generated block. The data storage query part on the chain consists of a structure and a storage query function which include course number and attributes of the data submitted by each participant.

4.4.2. Check score.
Scores of each subject can be obtained through the user interaction interface, and the inverted index is used to store scores, which improves the retrieval efficiency of scores. The index structure is shown in Figure 3 below.
4.4.3. Database module.

Our system adopts distributed data storage environment constructed by blockchain system, and provides powerful database access capabilities with cloud computing. Data changes are catalyzed by insert or update. Each change is assembled into a data block through encryption and submitted to the database. Through the verification of changes by multiple nodes, the authenticity of the data is jointly maintained and the data cannot be tampered with. Figure 4 shows a diagram of data structure which stored in the MySQL cloud database.

5. System operation results and analysis

We evaluated the system described in this article in terms of feasibility and tamper resistance.

5.1. Feasibility.

In the process of uploading the scores, the system calls the smart contract to save the data to the blockchain and obtains a summary. Demander checks the authenticity of the scores based on the summary. The system calls the comparison of contract-related data through the score summary. The traceability score data can verify whether the data information has been tampered with. If the data information of the traceability data is consistent with the hash value of the data information in the summary query, it can prove that the data has not been tampered with, the score is valid. If the score information queried from the blockchain during verification is empty, the submitted query is not valid.

5.2. Tamper-proof.

We also compared the system described in this paper with the system [9–10] anti-tampering scheme proposed by SUN Yun-qiu and GUO Hui-fang, and the result is shown in Figure 5. It shows that the
system described in this article provided better anti-tampering modification. With the increase in the number of change applications, the possibility of data being attacked increases and the anti-tampering ability of the other two systems will gradually decrease.

Figure 5. Degree of tamper-proof in three systems.

6. Conclusion
The student achievement protection system based on blockchain technology described in this article is a distributed data sharing service system through Ethereum. The system packs the data into blocks after being uploaded to the chain to ensure data traceability; Important data input and inquiries are obtained from the block chain to ensure that it cannot be tampered with and is true and reliable. Through smart contracts, it is transparent to users and provides high reliability while reducing the complexity of the system, which has a certain promotion value.

References
[1] Berner, M.M. (1993) Building Conditions, Parental Involvement, and Student Achievement in the District of Columbia Public School System[J]. Urban Education, 28(1):6-29.
[2] Zhang, C.C., Zhang L.L., Shi Y.Y. (2016) Design and Implementation of Student Achievement Management System Based on Android[J]. Modern Computer, 15.
[3] Wu Shuangke. CReam. (2019) A Smart Contract Enabled Collusion-Resistant e-Auction[J]. IEEE Transactions on Information Forensics and Security, 14(7): 1687 – 1701.
[4] Hisham S. Galal, Amr M. Youssef. (2019) Full Privacy Preserving Vickrey Auction on top of Ethereum[EB/OL]. https://arxiv.org/pdf/1905.06280v1.pdf.
[5] Yu Y, Li Y.N, Tian J.F. (2018) Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things[J]. IEEE Wireless Communications, 25(6):12-18
[6] Claudia Pop , Tudor Cioara , Marcel Antal. (2018) Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids[J]. Sensors, 18(1):162-183.
[7] Haya R. Hasan, K.Salah. (2019) Combating Deepfake Videos Using Blockchain and Smart Contracts [J]. IEEE Access, (7): 41596 – 41606
[8] Bertoni G , Daemen J , Peeters M . (2013) Keccak[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin. pp. 165-171
[9] Sun Y.Q., Wang Q.C. (2015) A college grade management system based on blockchain technology[J]. Journal of Cryptography, 005:568-578.
[10] Guo H.F., Wang Z.P., Liu H.B. (2020) Design of a trusted college student record system based on blockchain[J]. Modern Computer (Professional Edition), 000(011): 92-97.