Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 202 (2022) 283–288

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Identification, Information and Knowledge in the internet of Things, 2021

Blockchain-Based Secure Sharing Mechanism of Online Education Data

Yaofei Wang[a,b], Qiurui Sun[a], Rongfang Bie[a,*]

[a]School of Artificial Intelligence, Beijing Normal University, Beijing, 100875, China
[b]School of Computer Information Management, Inner Mongolia University of Finance and Economics, Hohhot, 010070, China

Abstract

The development of online education has broken the limitations of traditional education in region and time, and promoted the reform of education. However, there are some problems in traditional online education, such as data island, lack of data sharing model and so on. This paper constructs an online education data management model based on blockchain technology, which solves the problems of trust authentication of online learning data and curriculum resources; We put forward the trust generation and security sharing mechanism of online education data, analyze its security, and realize the security sharing of online education data on the basis of privacy protection.

Keywords: Blockchain; Online education; Data sharing; Security; Privacy protection;

1. introduction

The occurrence of COVID-19 has greatly highlighted the significance of online education popularization and application. The development of traditional information technology in teaching resource storage, virtual scene and teaching interaction provides an important support for the popularization and promotion of online education. According to the statistical data released by UNESCO on April 5, 2020, affected by the epidemic, 1.59 billion students, accounting for 91.3% of the total number of students in the world, cannot return to school. In this special case, students have to use online learning. However, in the existing online education model, there are still major challenges in data security, copyright protection, teaching evaluation, and effective utilization of teaching process data:

* Corresponding author. Tel.: +86-010-5880-4050. ; fax: +86-010-5880-4050.
E-mail address: rfbie@bnu.edu.cn

1877-0509
10.1016/j.procs.2022.04.037

- There are security risks in online education data. With the continuous development of online education, online education in Colleges and universities is gradually popularized in exploration. However, students use the online education platform to share a large amount of personal data, and the security of these data is very important. In 2020, Unacademy Platform, one of the largest online education platforms in India, has about 22 million user data sold on hacker websites and more than 500000 zoom account information sold on dark networks. These events show that online education data protection is imminent. It is listed by UNESCO as one of the biggest challenges facing the world.
- There is a lack of on and off chain data interaction mode of online education data. At present, blockchain technology is mainly used in five scenarios: digital currency, financial asset transaction settlement, digital government, certificate deposit anti-counterfeiting and data service. In the future, the Internet, artificial intelligence and the Internet of things will generate massive data. The existing centralized data storage mode will face great challenges. Edge storage computing based on blockchain technology is expected to become a solution. Online education data has the following problems: data source dispersion, the data index is not uniform, and the data analysis efficiency is low. Combining online education with block chain technology can solve the above problems well. However, in the process of combining online education data with blockchain technology, there is a lack of unified mode of data interaction on and off chain. This directly leads to the low efficiency of data security sharing based on blockchain, which is a major challenge restricting the application of blockchain technology in the field of online education.
- Contradiction between data privacy protection and data sharing efficiency. In the online application of colleges and universities, a large amount of data is controlled by the online education platform. There are some problems between the platforms, such as low data quality, data island, inadequate data security management, poor data circulation and sharing, etc. There are some problems in the process of data generation and collection of online education data, such as non-standard collection, excessive data collection and so on; There are some problems in data storage, such as data theft, data destruction and so on; There are some problems in data application, such as illegal data sharing and illegal transaction, which seriously restricts the rational sharing and application of online education data.

As a credible value delivery system, blockchain technology can effectively authenticate and store online education processes and resources, and promote the creation and dissemination of knowledge value. This paper proposes an online education data security sharing mode, and completes the online education data security governance system based on blockchain.

2. Related Work

Since Satoshi Nakamoto proposed to take blockchain as the core technology of bitcoin system in 2008 [1], blockchain, as a decentralized, tamper proof, secure and trusted technology, has been widely used in various fields.

In 2016, Sony announced that it had developed an internal certificate issuance system using blockchain technology. On August 10, 2017, Sony Corporation and Sony Global Education announced the development of a system to apply blockchain technology to the field of education. This system adopts the technology of “open and safe mutual use of educational achievements and activity records”, and centrally manages the data of multiple educational institutions, making it possible to record and refer to educational data and digital transcripts [2]. These two systems only realize the “write-into-chain” of education process data, and do not make further use of the on-chain data.

Turkanovi ć Muhamed proposed a global higher education credit platform called EduCTX. The platform is based on the concept of the European credit transfer system (ECTS). It constitutes a globally trusted and decentralized higher education credit and scoring system, which can provide globally unified data for students, higher education institutions (HEIS) and other potential stakeholders (such as companies, institutions and organizations) [3]. Genadijs gromovs (2017) introduced the development and evaluation process of higher education learning plans. The study points out that it is difficult to update the research scheme in terms of innovative technology trends in relevant knowledge fields [4]. Guang Chen focused on its potential educational applications and discussed how to use blockchain technology to solve some educational problems [5]. Chuyang Li proposed a digital rights management system supported by blockchain, which includes a new network architecture to share and manage online education multimedia

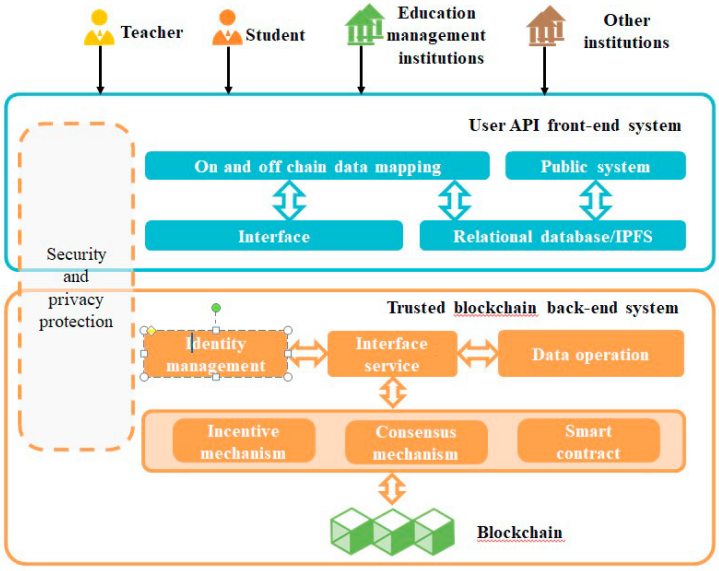

Fig. 1. Online education data security sharing management model.

resources on the basis of the combination of public and private blockchain; In addition, it also includes three specific smart contract schemes, which respectively realize multimedia digital copyright recording, secure storage of digital certificates and intermediary free verification [6]. Fadlil et al. Studied using blockchain to conduct online pocket money recharge transactions for students, and used AES encryption method for each block sequence to improve the security of transaction information [7]. Based on the education plan, Guustaaf discussed several higher education projects based on blockchain, and compared the differences and connections between the functions of blockchain currently used and existing education projects, and improved the implementation scheme of blockchain technology [8]. The above research does not discuss the data mapping mechanism on and off chain in detail, and does not consider the security problems encountered in data sharing.

3. Construction of online education data management model based on blockchain Technology

In the online education application scenario, the system needs to meet the different use needs of multiple roles such as teachers, students, and teaching management institutions at the same time. In the distributed storage process, it needs to maintain and manage various educational materials, certificates and other diversified digital files generated in the online education process, and ensure the normal implementation of various complex education and teaching businesses, This makes the traditional blockchain system structure with single role, fixed storage content and simple transaction logic incompatible with the online education environment. According to the actual application scenario of online education, the appropriate blockchain structure is designed, and combined with the characteristics of the application environment with multiple types of online education roles, diverse storage data types and diversified execution services, a global distributed online education data security sharing management model of colleges and universities is constructed. As shown in Figure 1.

User API front-end system: users access the system through the front-end web interface for operation. They will access the relational database or interact with the back-end blockchain through the public system or on and off chain data mapping. According to different user permissions and business operations, the generated process data will be divided into chain data (such as user node information, student achievement, educational resource data summary and other data requiring trusted management) and off chain data (such as cached data generated by user temporary query, educational resource original file, etc.). In the front-end system, the data mapping part on the chain realizes the mapping between the data summary on the chain and the database data, while the public system is used for the storage

and interaction of off chain data in the relational database. The combination of the two division of labor is used to manage the data, so as to effectively ensure the speed of system operation and save the storage space of the blockchain. Also, other organization can realize the trusted verification of data through the smart contract of the front-end system.

Trusted blockchain back-end system: including consensus mechanism, incentive mechanism, smart contract deployed by management organization, user node identity management and data operation. The interaction with users and the execution of actual business can be realized by the data mapping on the chain of the front-end system through the interface. Among them, the identity management operation and data operation of user nodes will trigger the incentive mechanism, consensus mechanism and smart contract of corresponding functions to jointly realize the block generation, consensus, trusted storage and secure sharing of underlying blockchain data summary information.

4. Security sharing mechanism of online education data based on smart contract

The secure sharing of online education data mainly includes the trusted production, storage security and secure sharing of online education data. The storage security can be realized through the blockchain system distributed storage system. Therefore, we mainly study the trusted production and secure sharing of data.

4.1. Online education data trusted write-into-chain

Data trusted production is mainly realized through self-authentication of online education data smart contract. Online education is different from classroom teaching based on physical object and on-site interaction. The teaching resources of educational institutions and the learning achievements of learners are presented in the form of various multimedia resources (for example, course videos, explanation audio, handout pictures, homework pictures and report videos submitted by learning users), And carry out necessary communication in the process of education through the transmission of the Internet. In this process, it is very important to ensure the originality of multimedia resources released in the system, which can effectively prevent the plagiarism, dissemination and illegal trafficking of multimedia teaching resources or learning achievements. Through the combination of tamper proof record of blockchain and digital watermarking technology, the digital copyright maintenance of multimedia education resources can be realized, and the data trusted authentication can be realized. The data write-into-chain process of smart contract is shown in Table 1:

Table 1. Data write-into-chain process.

Data write-into-chain process	//Resource data or learning process data (*t*)
1 if isResourceData(data)	
2 M = Hash(data);	//data is resource data
3 if isExistence(M);	
4 return;	//M is already in the blockchain
5 else	
6 writeblock(M);	//write the Hash of the resource data into the blockchain
7 else	
8 if size(data) ¡ Q	//Q is the threshold of data volume
9 return;	// The learning process data is not written into the chain temporarily
10 else	
11 writeblock(Hash(data));	//write the Hash of the learning process data into the blockchain
12 end	

For the multimedia teaching resources of the online education system, compare whether they are original through the hash value. If they are original, record the hash value on the chain, generate the corresponding certificate for the data through the smart contract, and record generation time, block location and other information. For online education process data, the amount of data is used as the trigger condition for write-into-chain operation. This interactive process is automatically completed by the system.

4.2. Secure sharing of online education data

The ultimate purpose of online learning data sharing is to facilitate third-party institutions to evaluate online learners without obtaining learners' specific learning data. We propose a third-party independent verification mechanism to achieve the above functions. Since the hash values of various digital certificates obtained by learning users in the online education system are publicly stored in the online education public chain / alliance chain, and the public keys of all educational institution users are also publicly disclosed in the whole system, it can be queried and verified by using the public key of educational institution users issuing the digital certificate and the personal public key of learning users with the certificate, The authenticity of any certificate information in the online education public chain / alliance chain can be directly verified. Based on this, a third-party independent verification mechanism of Digital Education Certificate in the process of entering a higher school and employment is formed. As shown in Table 2 and 3:

Table 2. Learner obtains verification code

Input: vpk	// visitor public key (*t*)
1 if isLearner(getid())	//learner identification
2 setTime(time);	//set temporary verification code aging
3 temv = Hash(vpk ¡¡ getCurrentTime())	//calculate temporary verification code
4 return temv;	

Table 3. The third-party independent verification process

Input: temv	//temporary verification code aging (*t*)
lpk	//learner public key
lipk	//Learning institution public key
1 if isLegaltem (temv) and isLegalpk(temv,getpk)	
2 return getdata(temy,lpk,lipk)	// Only when the visitor's public key and verification code are correct can they be verified

In order to protect the privacy of learners, only the third-party organization authorized by learners can access and verify their learning data. Learning users can generate temporary verification codes for their data in the system and invite third-party institutions to visit the online education public chain / alliance chain to verify their online learning data. The third-party institution can easily verify the correctness of learners' online learning information through the temporary verification code, the learning user's personal public key, and the public key and certificate block ID of educational institution users available in the system. The verification code generated in the verification process is temporary. If the user does not provide the verification code, other users will not be able to access the specific user certificate information, which not only protects the user's privacy, but also establishes a reliable bridge for the communication between third-party institutions and learning users.

5. Safety analysis

Data sharing security requires that the user data on the chain is safe, reliable and trusted. The data that users need to share can be queried by the receiver. Malicious users cannot obtain the corresponding user data by obtaining the information on the chain.

- The data on the chain is safe and reliable. Resource data and learning data are stored on the chain after consistency hash. The characteristic of consistency hash algorithm is that it can not deduce its original data from the data after hash, so as to ensure the security of data. At the same time, the original data are all online education process data. After reaching a certain amount, they are automatically linked through the smart contract to ensure the reliability of the data.

- The data that users need to share can be shared. Through the temporary verification code, the learner's public key, the learning institution's public key and the visitor's public key, the third-party institution can realize the normal access to the user's data by verifying the smart contract.
- Malicious users cannot get user data. The temporary verification code matches the public key of the third-party institution and has time limit. Even if it obtains the temporary verification code, it needs to log in to the account of the third-party institution before it can access user data, which further increases the cost for malicious users to obtain data.

6. Conclusion

Aiming at the problems of online education data island and lack of data sharing mode, this paper constructs an online education data management model based on blockchain, which solves the problems of online education resource data and online learning data write-into-chain authentication and storage in blockchain. Based on the temporary verification code and the third-party public key, an online education data sharing mechanism based on smart contract is proposed, and the effectiveness of the mechanism is verified by security analysis.

Acknowledgements

This research is sponsored by National Natural Science Foundation of China (No. 62177007, 61571049) and Industry-University-Research Innovation Foundation of Chinese University.

References

[1] Nakamoto S. (2008) "Bitcoin:A Peer-to-Peer Electronic Cash System." *Online* bitcoin.org/bitcoin.pdf.
[2] Sony.(2017) "Sony develops system for authentication, sharing, and rights management using blockchain technology" *Online* https://www.sonyged.com /2017/08/10/news/press-blockchain/.
[3] Turkanović Muhamed,Hölbl Marko,Košič Kristjan,Heričko Marjan,Kamišalić Aida. (2018) "EduCTX: A blockchain-based higher education credit platform,Digital Object Identifier"
[4] Genadijs Gromovs,Mika Lammi(2017) "Blockchain And Internet Of Things Require Innovative Approach To Logistics Education" *Transport Problems* **12** (2): 23–34.
[5] Guang Chen, Bing Xu, Manli Lu and Nian-Shing Chen (2018) "Exploring blockchain technology and its potential applications for education" *Smart Learning Environments* **5** (1): 1.
[6] Li Chuyang , Guo Junqi , Zhang Gguangzhi , et al (2019) "A Blockchain System for E-Learning Assessment and Certification",*2019 IEEE International Conference on Smart Internet of Things*, Tianjin, China
[7] Fadlil A , Riadi I , Nugraha N Toro A (2021) "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification" *Lontar Komputer Jurnal Ilmiah Teknologi Informasi* **11** (3): 155–166.
[8] Guustaaf E , Rahardja U , Aini Q , et al.(2021) "Blockchain-based Education Project" *Aptisi Transactions on Management (ATM)*, **5** (1): 46–61.