# A Method for Sharing of University Digital Resources Based on Alliance Chain

Yicai Wang

wangyicai@sdupsl.edu.cn

Network Information Center, Shandong University of Political Science and Law ,Jinan, China

**Abstract.** The sharing of digital educational resources in colleges and universities still faces challenges such as high cost, security problems, and inconsistent standards. The decentralized, immutable and traceable characteristics of blockchain technology are of great significance to solving these problems and educational resource sharing can be realized through its distributed ledger and security mechanism. Aiming at the above problems, in this paper, a method of university digital resource sharing is proposed based on alliance chain with identity authentication, resource sharing, privacy protection and value exchange as the main characteristics. Through the alliance chain technology, using its permanent record and immutable characteristics to achieve efficient digital resource management; Combine the semi-centralized consensus architecture of alliance chain and hierarchical node design to realize efficient resource sharing circulation and management; Based on smart contract and digital signature technology, data access and sharing can be de-trusted and intelligent. Experimental results show that the resource sharing model based on alliance chain technology can achieve good results in the sharing of academic digital resources within and among universities.

**Keywords:** blockchain; alliance chain; digital resources; sharing; smart contact

## 1. Introduction

The decentralization, immutable, traceability and other characteristics of blockchain technology are of great significance to solve the problem of digital educational resource sharing in universities, and educational resource sharing can be realized through its distributed ledger and security mechanism. At present, blockchain technology has been applied in the development of digital educational resources sharing in colleges and universities, such as the establishment of a digital textbook management system based on blockchain technology, and the development platform of digital textbooks based on digital textbooks[1]. However, the platform has some problems, such as high cost of platform development, lack of unified standard, high cost of development and high risk of information security[2]. At the same time, the application of existing blockchain technology in the field of digital educational resource sharing is mainly concentrated in the field of academic exchange and educational big data analysis[3], and it fails to combine it with the development of digital educational resources in colleges and universities[4].

EIMT 2024, March 29-31, Wuhan, People's Republic of China

DOI 10.4108/eai.29-3-2024.2347691

Therefore, in the context of blockchain technology, combined with the needs of the development of digital educational resources in colleges and universities, it is particularly important to explore the key issues in line with the sharing mode of digital educational resources in colleges and universities. On the one hand, blockchain technology can effectively integrate, classify and manage the digital educational resources formed by various universities. On the other hand, blockchain technology can solve the problems of high cost and low efficiency in the development of digital educational resources in colleges and universities.

## 2. Related Work

In the development of college education informatization, the digital education resource sharing platform of colleges and universities mainly includes learning platform, course platform and resource platform, aiming to realize the sharing of high-quality digital education resources and ensure the quality of education and teaching[5]. It is found that the current digital educational resource sharing platforms mainly have the following problems[6]:

- The existing digital education resource sharing platform has prominent information security problems. At present, the digital education resource sharing platform in colleges and universities generally has problems such as insufficient data security management measures and user information leakage, which seriously affect the user experience and use efficiency. In the process of sharing resources, the server may be destroyed or data lost due to network attacks. In addition, due to the sharing of teaching resources, user privacy is also threatened to some extent. Secondly, the copyright of resources. The publication of some digital works leads to great difficulties in the identification of resource copyright and subsequent rights protection [7]. Many teachers are worried that the copyright of the teaching content written by themselves will not be guaranteed after it is made public, which will make many high-quality teaching resources not be effectively used.
- Colleges and universities have different focuses on the development of digital educational resources, but they lack unified standards and norms.The digital resources of colleges and universities are mainly composed of libraries, educational technology centers and other departments. The separate management of multiple departments leads to scattered storage of resources and diversified platforms, and it is difficult to manage information resources in a unified way, which undoubtedly increases the burden on learners and makes them unable to find learning resources conveniently and quickly. In addition, coupled with the lack of communication within the departments, it is easy to cause duplication and waste of resources.

The integration of blockchain technology and digital educational resource sharing platforms in universities has great potential. From the perspective of the development trend of education informatization, the digital educational resource sharing platform of colleges and universities is an important infrastructure for the development of education informatization, which can provide various educational resources and services for colleges and universities, and help promote the sharing of high-quality educational resources.

## 3. Resource Sharing Based on Alliance Chain

Based on the above analysis, it can be seen that the development of digital education resource sharing platform in universities under the background of blockchain technology should have the following functions: First, the identity authentication. Through the blockchain technology to achieve the authentication of university digital educational resources user identity and related information; The second is the information security. Encrypting user data through blockchain technology to ensure that users' personal privacy is not infringed; Finally,it is the value exchange . All kinds of digital educational resources are classified and managed and shared through blockchain technology.

### 3.1 Blockchain Technology

Blockchain is a chain of blocks. Each block contains certain information, and they are connected into a chain in the order they are generated. Each block mainly consists of two parts: the block header and the transaction in the block. The block header contains the version number, previous block hash, Merkle root, timestamp, difficulty value, and random number [8].

Technically, blockchain is a distributed database designed to ensure data consistency among untrusted nodes and prevent tampering. Credit and records are stored on the blockchain, with each new block containing the digital fingerprint of the previous block, credit and records of its own, as well as a timestamp. This ensures that the blockchain continues to grow securely without being tampered with. Any modification to information in a block will render subsequent blocks' digital fingerprints invalid. The chained data structure makes it difficult to alter the history of the blockchain, requiring consensus mechanisms for maintaining data consistency among untrusted nodes.The structure of the block is shown in Figure 1.

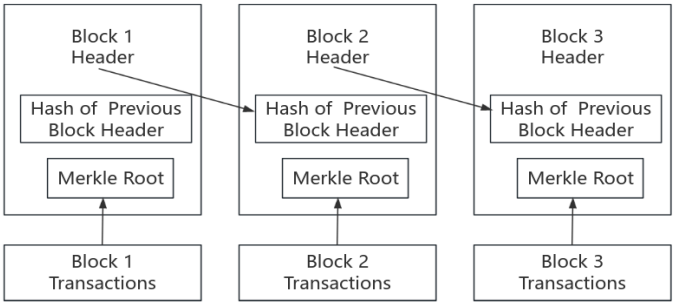


**Figure 1.** The structure of the block

Consensus mechanisms are predefined rules by which networks determine the authenticity of each record and block. Only those deemed true pass through and get recorded in the blockchain; otherwise, new blocks failing consensus mechanisms will be rejected by the network, rendering their information unrecognized.Common consensus mechanisms include PoW (proof of work), PoS (proof of stake), PBFT (practical Byzantine fault tolerance), etc., with PoW and PoS

currently being mainstream algorithms for encrypted digital currencies. Other common consensus mechanisms include DPoS and PBFT.

The working process of a blockchain mainly involves these steps:

- A sending node broadcasts new data records across the entire network.
- Receiving nodes verify received data record information for legality before including them in a block.
- All receiving nodes execute consensus algorithms (e.g., proof-of-work or proof-of-stake) on blocks.

Compared with the public blockchain in which any role is a part of the network and participates in the verification of transactions, although the degree of decentralization is weakened, the alliance blockchain divides the nodes in the chain in the form of an organization, which simplifies the communication structure and effectively improves the communication efficiency. The communication between internal nodes belonging to an organization is only carried out within the organizational network area. When cross-organizational consensus communication is needed, the communication is carried out through the anchor node selected in the organization during network construction. This enables the network delay to be controlled within the tolerable range when a large number of transactions are managed. Compared with the public chain, which relies on a large amount of computing power and time for transaction verification, the throughput rate of the alliance chain system is greatly improved[9].

### 3.2Access Authentication

User authentication refers to the authentication process of each participant in the digital education resource sharing platform. In the digital education resource sharing platform, users can submit the necessary identity information to the platform for identity authentication through smart contracts through authorization. In the process of identity authentication, it is necessary to identify and confirm the user's identity to ensure the authenticity and integrity of user information, and then ensure the security of the digital education resource sharing platform.

First, in smart contracts, user identity information can be stored. The immutability and distributed storage of blockchain technology enable user information to be verified and saved. At the same time, smart contracts can encrypt the user's identity information and store it in the blockchain[10]. Only authorized users can access these resources and perform related operations. In this process, the smart contract ensures the authenticity and integrity of user information by verifying the user's real identity information. Secondly, the authorization and management of resource sharing can be achieved in smart contracts. At the same time, data sharing can be managed and controlled through smart contracts, thus guaranteeing data integrity and security[11].

Rights management refers to authorizing resources and services in the system so that participants can access and use them. Rights management mainly includes the following two aspects:

1) request of Permissions: According to the permissions application strategy, the platform will review the applications of all participants, and only after the approval can it proceed to the

next step. In this part, each participant needs to complete certain operations to obtain the corresponding rights.

release of Permissions: When the permissions corresponding to a role is granted, a request is sent to other roles to release the corresponding permission. During this process, a role can initiate a request only after obtaining the corresponding permission. In this section, a role must complete certain operations before it can initiate a request to another role.

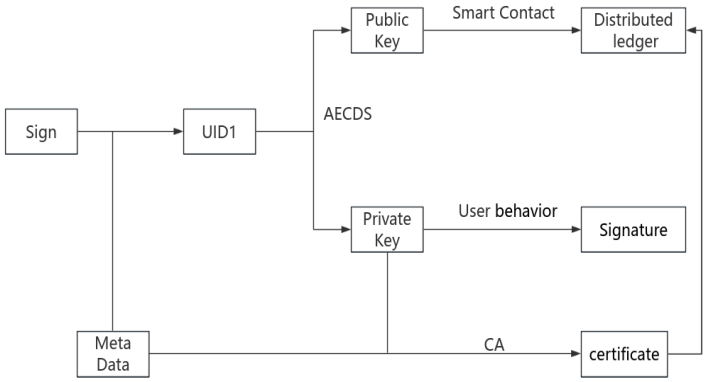


**Figure 2.** Access Authentication.

The digital education resource sharing platform allows different groups including students, teachers, enterprise employees, and other people to access the platform and set different permissions. Figure 2 shows the user identity authentication process.

### 3.3Data Exchange and Governance

Data exchange refers to the exchange and governance of data between different participants through blockchain technology. In the process of data exchange and governance, it is necessary to involve user identity information, business data and personal privacy information. Since there are different business types among different participants, relevant information needs to be authorized or decrypted according to actual business needs after data exchange and governance[12].

For users, they can access personally identifiable information, resource and personal privacy information on the digital education resource sharing platform through authorization[13]. After the completion of data exchange and governance, users can obtain the corresponding benefits, and will not suffer losses . For the platform, it is necessary to complete the processing of business data and personal privacy information on the user's authorized access to the digital education resource sharing platform, and store the relevant processing results in encrypted form on the blockchain. After the completion of the processing, the processing results and related privacy information need to be packaged to generate a new encrypted digest based on the blockchain consensus algorithm, and sent to the blockchain for verification and signature. The

user can then earn the corresponding revenue by earning revenue.Figure 3 shows Overview of digital resource sharing process

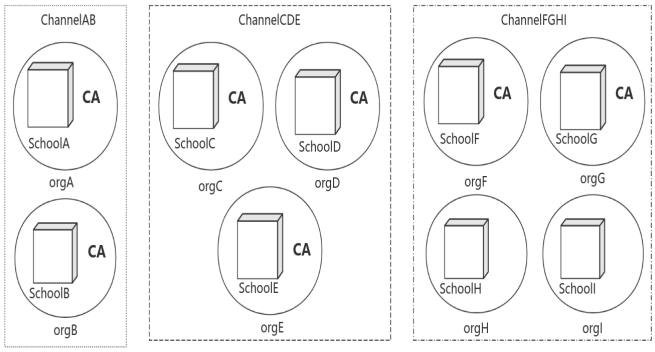


**Figure 3.** Overview of digital resource sharing

### 3.4Privacy Protection

In the process of digital educational resources sharing, data exchange and governance not only need to ensure the security of the participants' identity authentication, authority management and data exchange and governance, but also need to ensure the confidentiality and integrity of the participants' data[14]. Therefore, it is necessary to introduce a privacy protection mechanism on the sharing platform to ensure that the personal information of the participants is not leaked. This privacy protection mechanism is mainly implemented in several ways such as homomorphic encryption.Homomorphic encryption is shown in Figure 4.

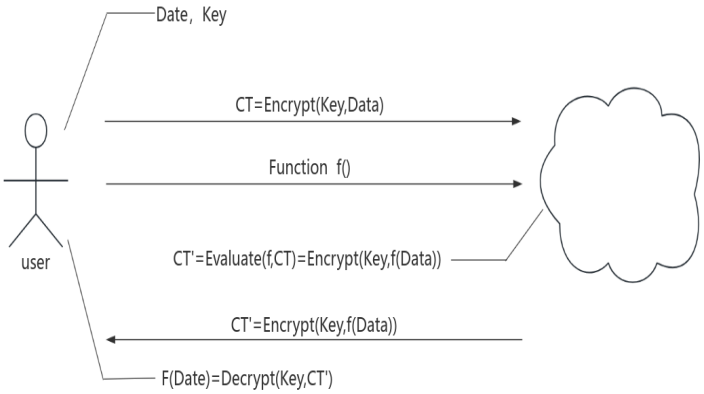


**Figure 4.** Homomorphic Encryption.

# 4. Experiments

## 4.1Experimental environment

In order to verify the feasibility of the university digital resource sharing scheme under the blockchain, this paper builds a prototype system to verify the feasibility of the scheme.The experimental environment of this paper is shown in Table I.

**Table 1**.Setup of experimental environment

| Experimental environment | Details |
|---|---|
| OS | WIndowsServer2012R2 |
| CPU | Inter(R) Xeon(R) Gold 5118 |
| RAM | 28G |
| GPU | Geforce RTX 3060 |
| Language | Java |
| Development Platform | Eclipse |

In the encryption process, SM2, Shamir, P2P and other related jar packages are introduced to build the alliance chain.

## 4.2Performance

The architecture of digital resource sharing in this paper is as follows: first, the creator publishes the digital educational resources that he will upload through through the smart contract deployed by the platform, and returns the corresponding resource hash value after the resources upload is successful, and stores the returned hash value in the blockchain.Second, the administrator audit resources through the platform.After the resources are approved successfully, they will be published on the platform successfully, and the database will be updated in time to ensure data synchronization.In the process of downloading resources, enterprises first realize resource link query, and finally sends a request to the database for resources.In the process of downloading resources, enterprises first realize resource link query, and finally sends a request to the database for resources.

System testing is mainly divided into functional testing and performance testing.Functional testing include data storage, query, update and delete operations, as well as the deployment and execution of smart contracts. Performance testing mainly include the response time and concurrency capacity of the system.

This paper designs three groups of experiments, respectively for 1024M, 256M and 128M file information for sharing, and adjusts the number of nodes accordingly. The results are shown in Figure 5.

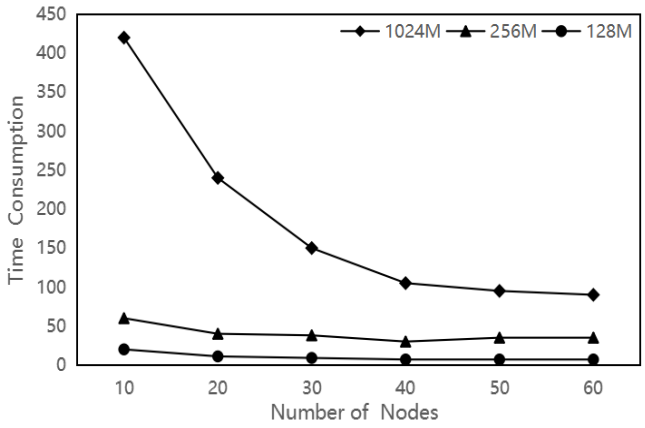


**Figure 5.** Results of Performance Testing.

As can be seen from the figure: the larger the amount of data, the more time is consumed; for each data level of sharing operation, the time consumption remains stable after the number of nodes increases to a certain amount. This is because in the transmission process, with the increase in the number of computing nodes, the data information will be divided into more small blocks for encryption operation, thus improving the operation speed. This paper tests the time required for data sharing under the condition of 3 to 50 participating nodes, which meets the requirements of real business scenarios. In summary, while meeting business requirements and security, the proposed model ensures system availability.

### 4.3Security

Security is an important evaluation index of digital resource management. In this paper, for resource sharing, the owner of the resource needs to store the data in the alliance chain in advance, and the integrity and privacy of the data are guaranteed by double-layer encryption and decryption.

If the proportion of abnormal data behaviors such as resisting external attacks is used as the analysis standard for security, the specific indicator is the ratio of successfully preventing abnormal data volume to all abnormal data volume. Use the Windows platform to build a blockchain development environment based on Ethereum, which contains 2 edge computing nodes and 15 terminal devices. Similarly, any 1MB of the above data is selected as the research object, and different methods are adopted to predict and prevent data attacks and theft in the process of data communication. The security results of the proposed method, asymmetric encryption method and classic blockchain method are obtained by comprehensive comparison, as shown in Figure 6.

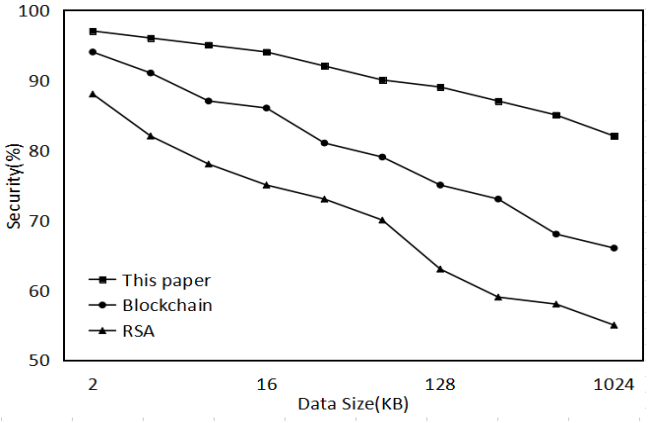


**Figure 6.** Results of Security Testing.

Compared with other methods, this method has the highest security. In terms of transaction verification, traditional secure multi-party computing has the risk of multiple nodes conspiring to tamper with data. After the introduction of blockchain, before traditional secure multi-party computing, a consensus algorithm is used to ensure the security and consistency of each blockchain node in the synchronization process, and then secure computing is carried out to ensure the security of the whole transaction process. In terms of security storage, the scheme adopts on-chain and off-chain common storage, corresponding to the data under the chain through the on-chain index, the information on the chain is stored on the block chain, all the index information has a time stamp to order the time and write into the block, and each block contains the information of the previous block. If you want to tamper with a piece of information on the block, at least 51% of the computing power is required, the data file is stored in the local database under the chain, so it ensures the security of the index information on the chain, so even if the file size reaches 1024kB, its security is not less than 80%. Methods based on classical blockchain technology only rely on a single model to process large amounts of data, so its security is difficult to guarantee. Similarly, asymmetric encryption methods only combine encryption technology and cannot exclude risks such as data tampering, so the overall effect is not good.

## 5 Conclusions

Applying blockchain technology to the field of digital educational resource sharing in colleges and universities can realize educational resource sharing through four aspects: identity authentication, resource sharing, privacy protection and value exchange. The application of blockchain technology can solve the problems faced in the process of digital education resource sharing, such as high cost, information security problems, and inconsistent resource development standards, and help build a safe and reliable digital education resource sharing platform for colleges and universities, and promote the efficient sharing of digital education resources.

However, it should also be noted that there are still some problems in the application process of blockchain technology, such as large security risks of blockchain data storage and difficult collaborative development of alliance chain members. Therefore, it is necessary to ensure the security of blockchain data storage from the aspects of underlying technical architecture and alliance chain node Settings. In the future, it is also necessary to further improve the application of blockchain technology in the sharing of digital educational resources in colleges and universities from the aspects of alliance chain node setting, data sharing and value exchange.

## References


[1] Du Pingping, and Li Yuke, "Research on Asset Storage and Data Reuse Rights License of Scientific Research Data in Colleges and Universities," Journal of Intelligence, vol.66(03), pp. 45–53,2022.

[2] Zhang Xueyuan, Du Pingping, and Lei Lei, " Research on the collaborative management of scientific experiment data based on blockchain technology,"Journal of Intelligence, vol.41(08), pp. 149–155,2022.

[3] Gu Ye, " Research and analysis on the security improvement of data center based on block-chain technology," Manufacturing Automation, vol.45(11), pp. 26–30,2023.

[4] Geng Qintao, and Yu Yangyang, "Research on searchable university data sharing scheme under blockchain," Computer Knowledge and Technology, vol.19, pp.77–80, August,2023.

[5] Cao Ning,, "Research on Data Resource Security Sharing Mechanism of Self-built Database of Library Based on Blockchain," Journal of Academic Library and Information Science, vol.41, pp.118–121, August,2021.

[6] Chen P W, Jiang B S, and Wang C H, "Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet," IEEE Computer Society, pp. 139–146, 2017 [Proceedings of the 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications].

[7] Hovland G, and Kucera J, "Nonlinear feedback control and stability analysis of a proof-of-work blockchain," Phil. Modeling, Identification and Control, vol.38(04), pp. 157–168,2017.

[8] Cai T, Lin H, and Chen W H, " Efficient blockchain-empowered data sharing incentive scheme for Internet of Things," Journal of Software, vol.32(04), pp. 953–972,2021.

[9] Janowicz K, Regalia B, and Hitzler P , " On the prospects of blockchain and distributed ledger technologies for open science and academic publishing,"Semantic Web, vol.5, pp. 545–555,2018.

[10] Song Jundian, Dai Bingrong, and Jiang Liwen, "Data governance collaborative method based on blockchain," Journal of Computer Applications, vol.38(09), pp. 2500–2506,2018.

[11] Wang Nan，Zhai Feng，and Cao Yongfeng, "Design of data sharing system based on blockchain technology," Science Technology and Engineering, vol.22(01), pp. 289–295,2022.

[12] [Huang Zhengzheng, and Zhang Xiaodie, "Design of knowledge sharing mechanism based on blockchain," Journal of Chongqing University of Technology(Natural Science), vol.35(09), pp. 143–151,2021.

[13] Wang Yihai, Liu Xing, "Research on Information Resource Sharing Model Based on Blockchain Technology," Informatization Research, vol.46(06), pp.1–6,2023.

[14] Zhong Siqi, Chu Chaochen,and Zhou Qin, "Analysis of Blockchain Application Models Based on Educational Resource Sharing," Computer Engineering, vol.52(11), pp. 78–80,2023.