Higher Educational Information Resource Sharing Model Based on Blockchain

https://doi.org/10.3991/ijet.v18i07.39241

Bing Dai, Xiaoguang An(✉)
Hebei Vocational College of Rail Transportation, Shijiazhuang, China
anlistone@163.com

Abstract—Through the sharing of high-quality educational resources in colleges and universities, various colleges and universities have carried out active and effective exchanges in teaching resources, avoiding the duplication of larger educational resources, and improving the academic and career development of teachers and students. The construction of a blockchain-based regional higher education information resource sharing model can solve the problems of scattered teaching resources and duplicate construction of teaching resources, difficulties to ensure the security of digital education resources, high operating costs of platforms, and urgent protection of intellectual property rights of resources. Most of the existing solutions rely on third-party certificate issuing centers or use a single key to encrypt the data flow of education information resources, which has hidden dangers of leakage of privacy information such as intellectual property rights, copyrights, confidential information of resources, other key information, and operation records. Therefore, this paper studies the regional higher education information resource sharing model based on blockchain and designs the data protection protocol of higher education information resources and its resource transaction relationship protection scheme. It introduces the blockchain-based regional higher education information resource sharing model mainly from three aspects: blinding the identity of authorized resource recipients, resource initiators publishing resource transactions, and authorized resource recipients publishing resource transactions. Experimental results verify the effectiveness of the proposed model.

Keywords—blockchain, regional higher education, education information resource sharing

1 Introduction

With the advancement of education informatization in China, it is necessary to build a digital education resource service system to achieve a balanced distribution of educational resources in colleges and universities of different regions and strengths, and truly realize educational equity [1–4]. Strengthening the sharing of high-quality educational resources in colleges and universities is of great significance to building a high-quality digital educational resource service system [5–9]. Through the sharing of high-quality educational resources in colleges and universities, various colleges and universities have carried out active and effective exchanges in teaching resources, avoiding the duplication of larger educational resources, and improving the academic and career development of teachers and students [10, 11].

The sharing of higher education information resources is of great significance to the society as well as teachers and students, but at present, there are mainly problems in four aspects: scattered teaching resources and duplicate construction of teaching resources, difficulties to ensure the security of digital education resources, high operating costs of platforms, and urgent protection of intellectual property rights of resources [12–17]. Combined with the advantages of blockchain, the construction of a blockchain-based regional higher education information resource sharing model can solve the above problems in a targeted manner. Carrying out relevant research not only plays a positive role in the promotion of China's education informatization, but also expands the application and development of blockchain in the field of higher education.

The rapid development of information technology has promoted the modernization of cross-language educational resource sharing. The educational resource sharing platform is the platform foundation for carrying out distance education activities, which is of great significance to the development of modern distance education. Yu and Jiang [18] carries out the hardware design of the cross-language education resource sharing platform, and designs the MCU controller in combination with the FPGA system to play a powerful control function. The design enables hardware connectivity based on resource reconfiguration ports and external input ports. Then, it designs the software of the cross-language education resource sharing platform, optimizes the resource sharing algorithm based on Hadoop framework, and enhances the multi-line sharing capability of the resource sharing algorithm. The development of the Internet of Things has brought convenience to people's lives, but the Internet of Things is facing severe challenges in the field of internal data sharing and educational information cache sharing. Wang [19] mainly studies the education information center network integrated resource cache sharing system based on the Internet of Things. Based on the school teaching management system and the lifelong education public service platform and combined with the actual situation of student information, the data management system of the online education information center analyzes the problems existing in the current workflow, then uses computer technology to standardize and convert the workflow, realizes the information of built-in resources in data management, and solves the problems of data cache sharing and data statistics in the management of the education information center. Zhu et al. [20] analyzes the problems existing in the co-construction and sharing of digital education resources in colleges and universities. Then, through the network structure of the blockchain, the model is built from an educational perspective. Building a university education resource sharing model based on blockchain technology can not only increase the sharing scope of educational resources, improve the quality of educational resources, but also protect the intellectual property rights of uploaders. In order to realize the unified organization and management of learning resources and improve the utilization rate of resources, Li et al. [21] proposes a design of mobile online education resource sharing system from the perspective of human-computer collaboration. It analyzes the main body and scope of collaboration, and builds a human-computer collaboration resource sharing model with large-scale human-computer collaboration as the main mode; defines system design principles, comprehensively considers the software layering idea and user usage, and determines the overall framework including the client, presentation layer and business logic layer; divides resource sharing into three stages: production, registration, review and release, and adopts "centralized management" to protect the intellectual property rights of distance education resources.

Although the existing blockchain-based regional higher education information resource sharing scheme improves the security of education information resource records and education information resource data storage in the regional higher education environment to a certain extent, most of the existing schemes rely on third-party certificate issuing centers or use a single key to encrypt the flow of education information resources, which has hidden dangers of leakage of privacy information such as intellectual property rights, copyrights, resource confidential information, other key information, and operation records. In addition, the problem of privacy information leakage brought about by the use of blockchain technology to implement access control has not been solved. Therefore, this paper studies the regional higher education information resource sharing model based on blockchain. In Chapter 2, this paper designs the higher education information resource data protection protocol and its resource transaction relationship protection scheme. In Chapter 3, this paper introduces the blockchain-based regional higher education information resource sharing model, which mainly includes three aspects: blinding the identity of authorized resource recipients, resource initiators publishing resource transactions, and authorized resource recipients publishing resource transactions. Experimental results verify the effectiveness of the proposed model.

2 Higher education information resources data privacy information protection scheme

In order to realize the sharing of higher education information resources, if the higher education information resource data is directly stored on the chain for sharing, any node in the network can obtain the higher education information resource data, and there is a greater risk of exposure to privacy data such as intellectual property rights, copyright, resource confidential information, other key information, and operation records. When the higher education information resource data is recorded through block resource transactions, there is still a risk of exposing private data if the relationship between the initiator and receiver of higher education information resource sharing in the resource transaction is not damaged. At the same time, higher education information resources have a large amount of data content and volume, so it is necessary to design a sharing scheme with higher security and less storage pressure. This paper designs the higher education information resource data protection protocol and its resource transaction relationship protection scheme.

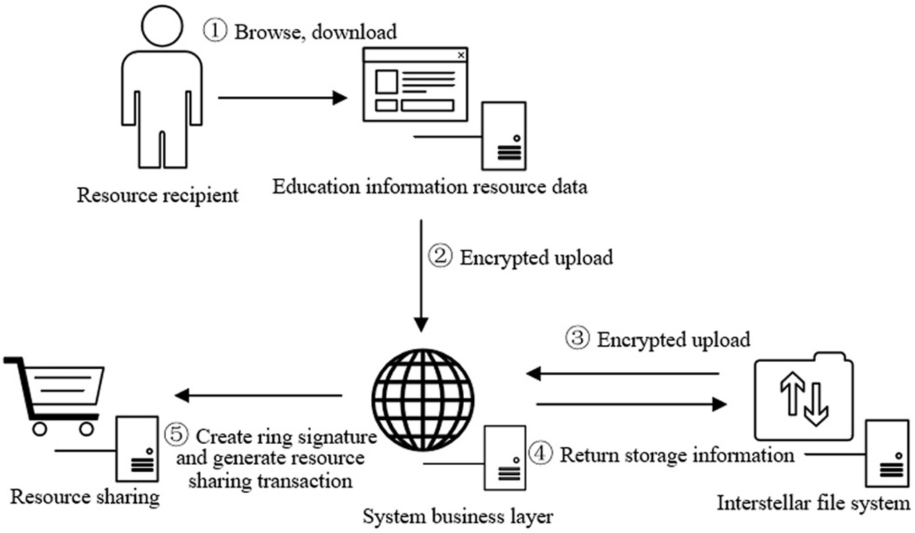

Fig. 1. Data privacy information protection process for education information resources

Figure 1 shows the process of protecting education information resources, data privacy, and information. In the higher education information resource data protection protocol, node *X* on the blockchain chain sends a message to node *Y* on the blockchain chain, which is represented by *X*→*Y*, the resource receiver is represented by *YS*, the resource initiator is represented by *BR*, the sharing system is represented by *GT*, the interstellar file system is represented by *XT*, the higher education information resource data generated by the resource receiver for the resource initiator is represented by *BS*, the information about the identity of the resource initiator is represented by *BX*, the public key of the resource initiator is represented by ol_o, the symmetric key of the resource initiator is represented by *l*, the identity of the initiator of obtaining resources and related keys are represented by *HM*, the ring signature created by the node of the academic affairs department of colleges and universities is represented by *QM*, the upload method of higher education information resource *BS* is represented by *SF*, the symmetric encryption method of higher education information resource *BS* is represented by *DJ*, the creation ring signature is represented by *CQ*, and the method of creating resource transaction is represented by *CJ*.

The specific protocol design is as follows:

1) $YS \rightarrow BR{:}HM(BX, ol_o, l)$// The resource recipient requests the identity and key from the resource initiator;
2) $YS{:}DJ\,(BS, l)$// The resource receiver uses the symmetric key of the resource initiator to encrypt the higher education information resource data to obtain the encrypted data T_{BL};
3) $YS \rightarrow GT{:}SF(T_{BL})$// The resource recipient uploads the higher education information resource data encrypted by the resource initiator to the sharing system;

4) $GT \rightarrow XT:SF(T_{BL})$// The sharing system uploads the encrypted higher education information resource data to the interstellar file system;
5) $GT \rightarrow XT:\{UT, UE\}$// After the higher education information resource data is successfully uploaded, the corresponding interstellar file system address and storage status are returned to the sharing system;
6) $GT:CQ\ (ol_C)$// The sharing system uses the public key of the academic affairs department of colleges and universities node to create a ring signature and record it in the resource transaction;
7) $GT:CJ(QM, ol_o, DW\}$// The sharing system creates a resource transaction based on the ring signature, the initiator's public key, and other auxiliary information and stores it in the resource transaction pool.

Since the initiator of the resource transaction needs to perform signature verification on the resource transaction in the resource transaction structure, the nodes participating in the signature generation mainly include signature nodes and ring member nodes. Therefore, combined with the ring signature, the resource transaction address of the node of the academic affairs department of colleges and universities that generates the resource transaction can be anonymized, thereby destroying the correspondence between the resource initiator and the academic affairs department of colleges and universities in the resource transaction and protecting the privacy of the resource initiator.

It's assumed that the message to be signed is represented by n, the public key of the node or resource initiator i is represented by ol/ol_i, the private key of the node or resource initiator i is represented by rl/rl_i, the set of signer public keys signed by the ring is represented by OL, the order corresponding to the base point of the elliptic curve is represented by H, the function of calculating the *hash* using the *sha*256 algorithm is represented by $QR()$, the ring signature calculation random number of the node or resource initiator i is represented by s_i, and the ring signature calculation scalar of the node or resource initiator i is represented by d_i. The set of random numbers of the ring signature is represented by S, the random number of the ring signature is represented by l, and the generated ring signature is represented by HQ. The following designs the initialization stage, signature generation stage, and signature verification stage of the algorithm.

In the initialization stage of the algorithm, when building the consortium chain, the consortium chain management node invites all academic affairs department of colleges and universities nodes to join the chain, and assigns key pairs (rl, ol) to all academic affairs department of colleges and universities nodes, wherein:

$$ol = rlH \tag{1}$$

The consortium chain management node transmits the key to the nodes of the academic affairs department of colleges and universities. When the resource initiator forms a new higher education information resource, the resource recipient can browse and download the higher education information resource and upload its behavior record, and when the behavior record is successfully uploaded to create a new resource transaction, the resource transaction initiator needs to be processed, the correspondence between the resource transaction initiator and the receiver is destroyed, and the sharing system enters the stage to generate signatures.

In the signature generation stage of the algorithm, it's assumed that the number of ring signature members is represented by *M*, the message to be signed is represented by *n*, and the key pair of the initiator of the resource transaction is represented by (rl_i, ol_i). When initiating a resource transaction, the sharing system randomly selects M–1 voting nodes as ring members for the initiator *FQ* of the resource transaction (usually the academic affairs department of colleges and universities), then the public keys of all ring members can be represented by $ol_i(jT[I,M])$, and the signer's public key ol_i is also included therein, forming the signer's public key set *OL* as shown in the following equation:

$$OL = \left\{ol_1, ol_2, ..., ol_{i-1},\ ol_{i-1}, ol_i, ol_{i+1}, ..., ol_{m-1}, ol_m\right\} \tag{2}$$

At the same time, the sharing system generates *M* random numbers for the construction ring signature:

$$S = \{s_1, s_2, ..., s_{i-1}, s_{i+1}, ..., s_{m-1}, s_m\} \tag{3}$$

Assuming the signer's public key is represented by ol_i, other public keys in the signer's public key set other than ol_i correspond one-to-one with each random number. Assuming there is a random number *l* and a scalar d_i, then:

$$lH = s_i H + d_i ol_i \tag{4}$$

Assuming that the public key in the signer's public key set is represented by ol_a, and both d_a and *l* are known, the ring signature recursive given by the following equation can be constructed:

$$d_a = QR(n, s_{a-1}H + a_{a-1}ol_{a-1}) \tag{5}$$

Recursive of the results of d_a based on the above equation is:

$$d_{i+1} = QR(n, s_i H + d_i ol_i) \tag{6}$$

After the calculation is completed, the ring signature $QM = \{d_i, OL, S, n\}$ can be generated based on *d*, *OL*, and *S*.

In the verification signature stage of the algorithm, when the validity of $QM = \{d_i, OL, S, n\}$ needs to be verified, the ring signature can be queried according to the resource transactions on the block, and verified based on the recursive verification equation shown in the following equation:

$$d'_{i+1} = QR(n, s_i H + d'_i ol_i) \tag{7}$$

If d_i *is* equal to d'_i, the signature is considered valid.

3 Construction of regional higher education information resource sharing model based on blockchain

Next, this paper introduces the blockchain-based regional higher education information resource sharing model, which mainly includes three aspects: blinding the identity of authorized resource recipients, resource initiators publishing resource transactions, and authorized resource recipients publishing resource transactions. Figure 2 shows the regional higher education information resource sharing process.

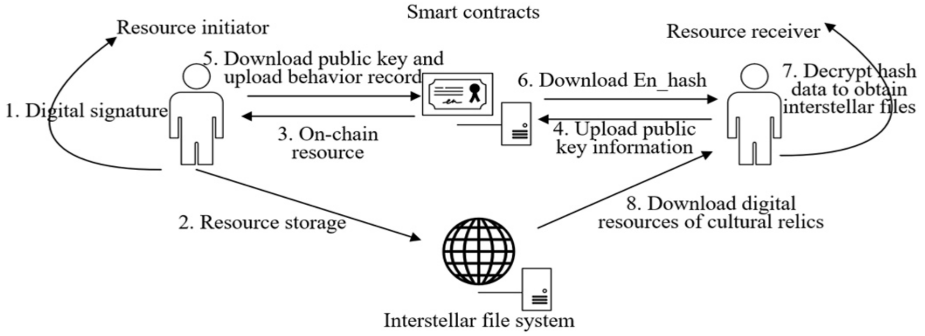
Smart contracts
Resource initiator
Resource receiver
5. Download public key and upload behavior record
6. Download En_hash
7. Decrypt hash data to obtain interstellar files
1. Digital signature
3. On-chain resource
4. Upload public key information
8. Download digital resources of cultural relics
2. Resource storage
Interstellar file system

Fig. 2. Regional higher education information resource sharing process

In order to avoid the leakage of the privacy information of the resource initiator due to the transparency of the blockchain. In this paper, the public key of the authorized resource receiver is blinded, and the resource receiver is authorized to use the blinded public key to publish resource transactions, and the blinded private key then generates the signature information in the on-chain resource transaction. This paper divides the public key blinding process into the following five steps:

1) Let the O-order prime addition cyclic group be represented by H, and the generator of H be represented by h, and choose the *hash* function $F{:}(0,1)\rightarrow c_o$. The resource initiator announces global parameters represented by $GP = \{H, h, O, F(.)\}$. The public and private keys of the resource initiator are represented by (OL_{RI}, RL_{RI}), and the public and private keys of the authorized resource recipients are represented by $(OL_{RR}, RL_{RR}\}$. The public key of the authorized resource recipients can be expressed as $OL_{RR} = h\cdot RL_{RR}$.
2) Determine the blinding factor, represented by s, and the resource initiator is randomly selected.
3) Set the blinded public key, represented by OL'_{RR}, as follows:

$$OL'_{RR} = OL_{RR} + s\cdot h = RL_{RR}\cdot h + s\cdot h = (s + RL_{RR})\cdot h \tag{8}$$

4) The resource initiator randomly selects s', $s' \in C_o$. The ciphertext D_1 and D_2 is generated through Elgamal encryption, and D_1 and D_2 are sent to the authorized resource recipient.

$$D_1 = s' \cdot h \tag{9}$$

$$D_2 = s + s' \cdot OL_{RR} \tag{10}$$

5) After the authorized resource recipient receives D_1 and D_2, it combines its own private key to calculate s by the following equation:

$$D_2 - RL_{RR} \cdot D_1 = (s + s' \cdot OL_{RR}) - RL_{RR} \cdot s' \cdot h = s + s' \cdot OL_{RR} - s' \cdot OL_{RR} = s \tag{11}$$

Substituting the calculated s into Equation 8 to obtain the blinded public key OL'_{RR} and the blinded private key $R'_{RR} = (s + RL_{RR})$. The authorized resource receiver can issue resource transactions based on OL'_{RR}, and RL'_{RR} is used to generate signature information.

In the process of sharing education information resource data, the resource initiator will publish two types of resource transactions to the blockchain, namely the resource transaction recording the hash value of encrypted education information resource data and signature information, which is represented by ea_{SJ}, and the resource transaction used to realize the sharing of education information resource data and the authorization and revocation of the resource recipient, which is represented by ea_{SH}. Assuming that the identity used to identify the resource initiator is represented by OL_{RI}, the time-stamp information of the published resource transaction is represented by ea_{SJ}, and the hash value of the encrypted education information resource data is represented by *JK*, stipulating that for every 10 pieces of education information resource data encrypted, the resource initiator publishes an ea_{SJ} on the blockchain, that's, *JK* includes $\{hash_{i+1}$, $hash_{i+2}$, ..., $hash_{i+10}\}$. The hash value of the resource initiator's identity OL_{RI}, timestamp information ea_{SJ}, and encrypted education information resource data is represented by ZD_{SJ}, the signature information is represented by *JK*, and the hash value of all fields in ea_{SJ} is represented by *WR*. At the same time, *WR* is used to establish the correlation between ea_{SJ} and resource transaction ea_{RU}, and the *WR* included in ea_{RU} is used to represent the basis on which authorized resource recipients can browse and download resource data. The ea_{SJ} content is given by:

$$ea_{SJ} = \{OL_{RI}, er_{SJ}, JK, ZD_{SJ}, WR\}$$

where,

$$ZD_{SJ} = \{RL_{RI}, F(OL_{user} \| er_{SJ} \| JK)\}, WR = F(OL_{RI} \| er_{SJ} \| JK \| ZD_{SJ}) \tag{12}$$

The resource initiator publishes education information resource data sharing resource transaction ea_{SH} on the blockchain to realize the sharing of education information resource data and the revocation and authorization of the resource recipient. Assuming that the identity of the resource initiator is represented by OL_{RI}, the timestamp information that publishes this resource transaction is represented by er_{SH}, the shared key that decrypts $TE(KE_{SH}, SHLI)$ is represented by KE_{SH}, the ciphertext obtained by the resource initiator using the blinded public key OL'_{RR} of the authorized resource receiver to encrypt $TE(KE_{SH}, SHLI)$ is represented by TE_{RR}, and the authorized resource recipient can decrypt TE_{RR} with its blinded private key RL'_{RR} to obtain $TE(KE_{SH}, SHLI)$. Then and the authorized resource recipient decrypts the $TE(KE_{SH}, SHLI)$ by using the shared key KE_{SH} in the education information resource data sharing resource transaction ea_{SH}, so as to obtain the token stored in the shared list *SHLI* to the authorized resource receiver. The authorized resource recipient then calculates the corresponding key based on the token, decrypts it, and then views the education information resource data shared by the resource initiator and makes a diagnosis. The identity OL_{RI} of the resource initiator in ea_{SH}, the timestamp information er_{SH}, the shared secret KE_{SH}, and the signature information of TE_{RR} are represented by ZD_{SH}, and the hash values of all fields in ea_{SH} are represented by *WT*. The ea_{SH} content is given by the following equation:

$$er_{SH} = \{OL_{RR}, er_{SH}, KE_{SH}, TE_{RR}, ZD_{SH}, WT\}$$

where,

$$\begin{aligned} &TE_{RR} = TE\{OL'_{RI}, TE(KE_{SH}, SHLI)\}, ZD_{SH} = \{RL'_{RR}, F(OL_{user} \| er_{SH} \| KE_{SH} \| TE_{RR})\} \\ &WT = F(OL_{RI} \| er_{SH} \| KE_{SH} \| TE_{RR} \| ZD_{SH}) \end{aligned} \tag{13}$$

The resource initiator implements authorization and revocation of the resource receiver by updating the blinded public key OL'_{RR} of the authorized resource receiver.

Before browsing and downloading resources, the authorized resource recipient needs to verify the signature information in ea_{SJ} and ea_{SH} to ensure that both ea_{SJ} and ea_{SH} are published by the resource initiator himself. The authorized resource receiver then decrypts the TE_{RR} using RL'_{RR} and KE_{SH} to obtain a shared list *SHLI* that stores the token. According to the token, the corresponding key stream fragment is obtained, and then the corresponding encrypted education information resource data is obtained from the cloud, and the hash value of the encrypted education information resource data is calculated and compared with the hash value stored in ea_{SJ}. If the hash values of the two parties are the same, it means that the education information resource data stored in the cloud has not been tampered with.

Finally, the authorized resource recipient uses the key stream fragment calculated by the token to decrypt and view the education information resource data shared by the resource initiator, and browse and download the resource. After that, the authorized resource receiver uploads the behavior record information to the cloud using key KE_{RU} encryption, and adds its corresponding hash value to the resource transaction ea_{RU} published by the authorized resource receiver. It's assumed that the blinded public key OL'_{RR} of the authorized resource recipient is used to identify the authorized resource recipient, and er_{RU} is the timestamp information of publishing the transaction of this resource. *PLG* is the hash value of encrypted resource browsing and downloading behavior information, and the digital envelope formed by the authorized resource receiver to use the key KE_{RU} encrypted with public key OL_{RI} of the resource initiator is represented by TE_{RI}, and ZD_{RU} is the signature information of OL'_{RR}, er_{RU}, *PLG*, KE_{RU}, TE_{RI} and *WR*. The hash values of all fields in ea_{RU} are represented by *WE*. Then the ea_{RU} content published by the authorized resource recipient is given as follows:

$$ea_{RU} = \{OL'_{RR}, er_{RU}, WR, PLG, TE_{RI}, ZD_{RU}, WE\}$$

where,

$$\begin{aligned} &TE_{RI} = TE(OL_{RI}, KE_{RU}), ZD_{RU} = \{RL'_{RR}, F(OL'_{RR}, er_{RU}, WR, PLG, TE_{RI})\} \\ &WE = F(OL'_{RR} \| er_{RU} \| WR \| PLG \| TE_{RI} \| ZD_{RU}) \end{aligned} \tag{14}$$

Figure 3 shows the system interaction diagram of the blockchain-based regional higher education information resource sharing model.

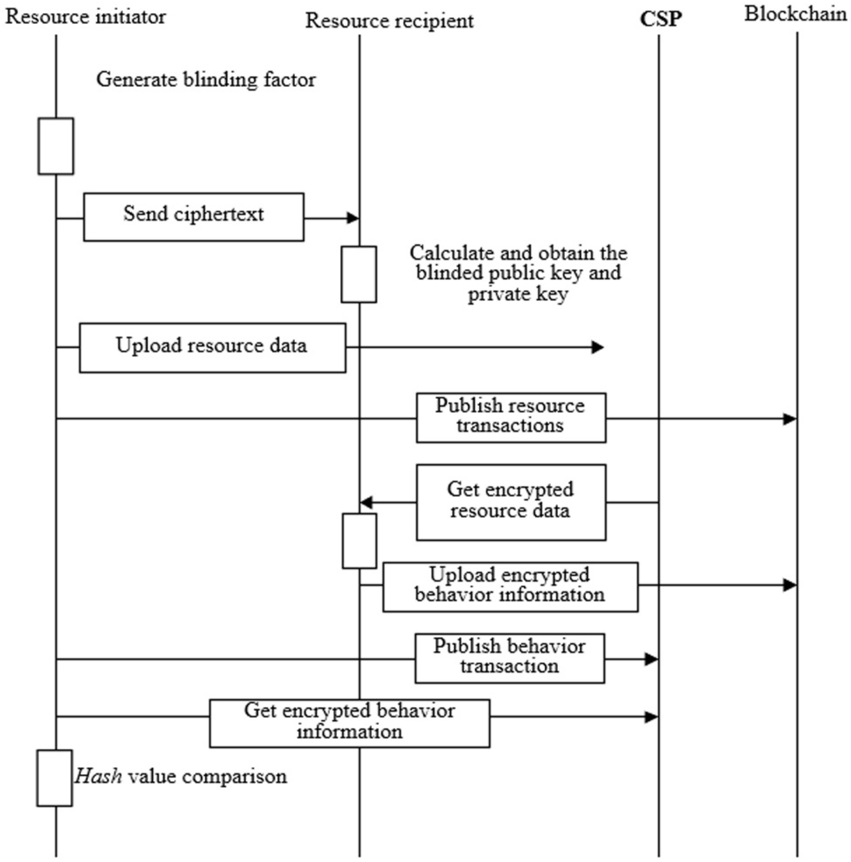
Resource initiator
Resource recipient
CSP
Blockchain
Generate blinding factor
Send ciphertext
Calculate and obtain the blinded public key and private key
Upload resource data
Publish resource transactions
Get encrypted resource data
Upload encrypted behavior information
Publish behavior transaction
Get encrypted behavior information
Hash value comparison

Fig. 3. System interaction diagram

4 Experimental results and analysis

The higher education information resource data privacy information protection scheme improves the fault tolerance rate of the higher education information resource sharing model by introducing signature verification of resource transactions. The voting nodes with the proportion *g* are randomly selected as ring members to construct the consensus group, which indicates that the remaining $(1-g)M$ nodes do not participate in the signature generation process, so the fault tolerance rate of the higher education information resource sharing model is increased to $(gM-1)/3+(1-g)M$. The experiment compares the fault tolerance rate of the consortium chain when g is 1, 0.9 and 0.8, that's, 100%, 90% and 80% of the voting nodes participate in the signature generation process, and the smaller the value of g is, the greater the fault tolerance rate of the consortium chain is. The comparison results of node fault tolerance rate of the higher education information resource sharing model are shown in Figure 4.

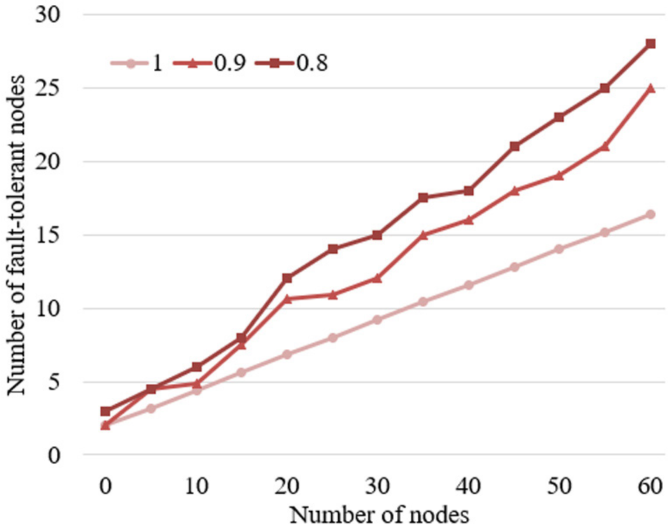

Fig. 4. Node fault tolerance rate of education information resource sharing model

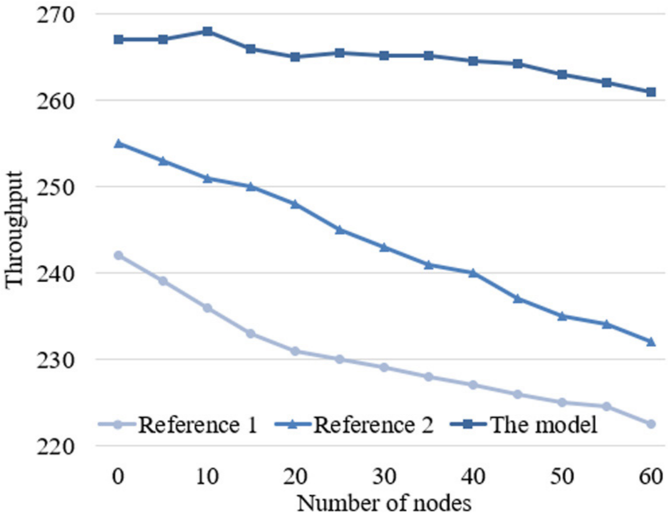

Fig. 5. Throughput of different models

In this paper, the *Caliper* test tool is used to compare the throughput of the shared model using the signature verification scheme of this paper when the number of nodes is 10, 20, 30, 40, 50, and 60 with the shared model using the *BLS* batch signature verification scheme (Reference 1) and the *ECDSA* signature verification scheme (Reference 2). The throughput of the three models is shown in Figure 5. It can be seen from the figure that the throughput rate of the sharing model shows an overall downward trend with the increasing number of nodes in the consortium chain. Among them, the throughput of the shared models using *BLS* batch signature verification scheme (Reference 1) and *ECDSA* signature verification scheme (Reference 2) decreases rapidly. Therefore, the shared model using the signature verification scheme in this paper is more suitable for scenarios with high throughput requirements than the other two reference models.

In order to verify the security of the higher education information resource sharing model proposed herein, this paper compares the proposed scheme with five reference schemes. A comparison is given in Table 1.

Table 1. Comparison of higher education information resource sharing schemes

	Blockchain	**Data Storage Location**	**Consortium Chain**	**Signature Verification**	**Lead-in Edge**	**Blind Public key**
Reference 1	√	Cloud-based	√	×	×	×
Reference 2	√	Private chain-based	√	×	×	×
Reference 3	√	Local server-based	√	×	×	×
Reference 4	√	Cloud-based	√	×	√	×
Reference 5	×	Cloud-based	×	×	×	×
The Model	√	Local server-based/ Edge server	√	√	√	√

Through comparison, it is found that the higher education information resource sharing model constructed herein has more advantages in data privacy protection and data security. Firstly, based on the higher education information resource data privacy information protection scheme, it ensures the integrity of data and private data such as intellectual property rights, copyrights, resource confidential information, other key information and operation records, and anonymizes the resource transaction address of the node of the academic affairs department of colleges and universities that generates the resource transaction, thereby destroying the correspondence between the resource initiator and the academic affairs department of colleges and universities in the resource transaction. Second, it blinds the public key of the authorized resource recipient to avoid the disclosure of the private information of the resource initiator due to the transparency of the blockchain. With the introduction of edge storage, the system can respond faster to requests from resource recipients. Finally, each access record such as browsing and downloading of the resource recipient is stored in the consortium chain. By establishing an authorization mechanism, it guarantees the privacy and integrity of resource data in the sharing process.

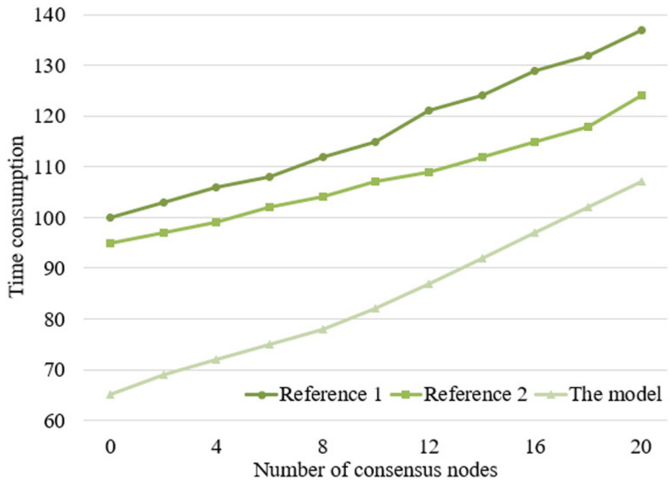

Fig. 6. Consensus time consumption

The time consumption of the higher education information resource sharing model proposed herein is compared with the sharing models using *PoA* consensus algorithm (Reference 1) and *PBFT* consensus algorithm (Reference 2). The experimental results are given in Figure 6. It can be seen from the figure that the time required for model nodes to reach consensus increases with the increasing number of consensus nodes. Since the communication overhead of node consensus of the higher education information resource sharing model proposed herein is smaller than that of *PoA* consensus algorithm and *PBFT* consensus algorithm, the consensus efficiency of this model is higher.

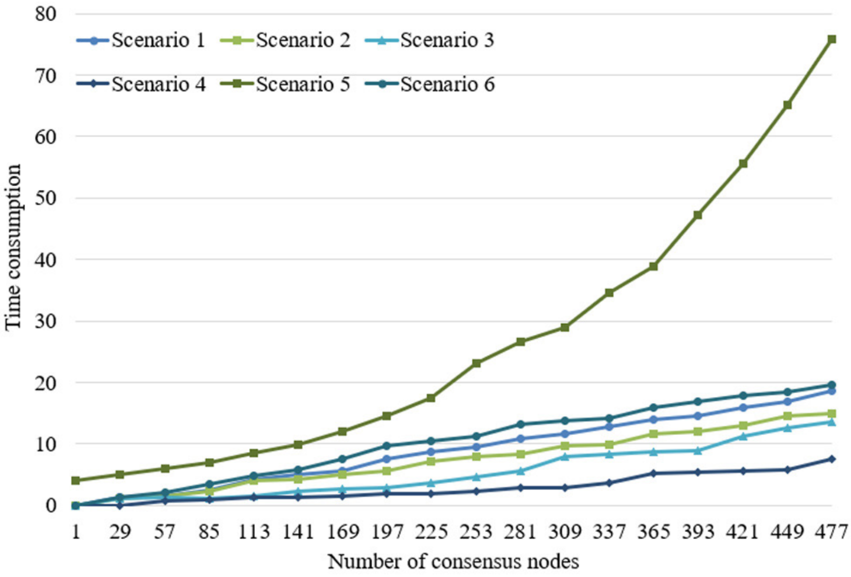

Fig. 7. Comparison of higher education information resource reading delay experiment

Taking the number of resource sharing transactions as variables, it compares the data reading latency of the six access situations of higher education information resource sharing (cross-regional local sharing, cross-regional non-local sharing, non-cross-regional local sharing, non-cross-regional non-local sharing, no cloud chain combination, and cloud chain combination) of this model with the comparison results shown in Figure 7. As can be seen from the figure, the resource data sharing delay increases with the increasing number of transactions. The proposed model encrypts and stores higher education information resource data in the cloud by combining cloud chain, which can achieve faster response to resource recipients' requests and obtain shorter data transmission time.

Table 2. The time cost of each stage of the consensus model herein

Encryption	Authentication	Consortium Chain Search	Re-encryption	Decryption 1	Decryption 2
7.54	0.45	6.62	6.75	7.13	10.34

Table 2 counts the time cost of each stage of the consensus model. Decryption 1 and decryption 2 represent *DO* and *DU* decryption of the re-encrypted ciphertext, respectively. In addition to the time cost of *DU* decryption exceeding 10ms, the operating cost of other stages such as encryption and authentication does not exceed 8ms.

5 Conclusion

This paper studies the regional higher education information resource sharing model based on blockchain and designs the data protection protocol of higher education information resources and its resource transaction relationship protection scheme. It introduces the blockchain-based regional higher education information resource sharing model mainly from three aspects: blinding the identity of authorized resource recipients, resource initiators publishing resource transactions, and authorized resource recipients publishing resource transactions. Combined with the experiments, it develops the comparison results of node fault tolerance rate of the higher education information resource sharing model, and the throughput of the sharing model using the signature verification scheme in this paper and the sharing models using the *BLS* batch signature verification scheme (Reference 1) and the *ECDSA* signature verification scheme (Reference 2). It is verified that the sharing model using the signature verification scheme in this paper is more suitable for scenarios with high throughput requirements than the other two reference models. By comparing this scheme with the five reference schemes, it is found that the higher education information resource sharing model constructed herein has more advantages in data privacy protection and data security. The time consumption of the higher education information resource sharing model proposed herein is compared with the sharing models using *PoA* consensus algorithm (Reference 1) and *PBFT* consensus algorithm (Reference 2), which verifies that the consensus efficiency of this model is higher. The comparison results of higher education information resource reading delay experiment verify that the proposed model can achieve faster response to resource receivers' requests and obtain shorter data transmission time.

6 References

[1] Jiang, X. (2022). Design of artificial intelligence-based multimedia resource search service system for preschool education. In 2022 International Conference on Information System, Computing and Educational Technology (ICISCET), Montreal, QC, Canada, pp. 76–78. https://doi.org/10.1109/ICISCET56785.2022.00027

[2] Cui, L. (2020). Research on the application of social network service in resource sharing of ideological and political education in colleges. In 2020 International Conference on Robots & Intelligent System (ICRIS), Sanya, China, pp. 210–213. https://doi.org/10.1109/ICRIS52159.2020.00060

[3] Wang, M., Guo, H. (2022). Informatization construction of physical education resources based on service-oriented architecture. Mobile Information Systems, 2022: 1447943. https://doi.org/10.1155/2022/1447943

[4] Zhang, J., Qi, T. (2022). Construction of educational resource metadata management platform based on service-oriented architecture. Journal of Sensors, 2022: 2172817. https://doi.org/10.1155/2022/2172817

[5] Bilyalova A, Bazarova L, Salimova D, et al. (2021). The digital educational environment: The problem of its accessibility for visually impaired students. International Journal of Emerging Technologies in Learning, 16(16): 221–230. https://doi.org/10.3991/ijet.v16i16.23453

[6] Wen, J., Wei, X.C., He, T., Zhang, S.S. (2020). Regression analysis on the influencing factors of the acceptance of online education platform among college students. Ingénierie des Systèmes d'Information, 25(5): 595–600. https://doi.org/10.18280/isi.250506

[7] Luo, Y., Yee, K.K. (2022). Research on online education curriculum resources sharing based on 5G and internet of things. Journal of Sensors, 2022: 9675342. https://doi.org/10.1155/2022/9675342

[8] Budiarti, M., Ritonga, M., Rahmawati, Yasmadi, Julhadi, Zulmuqim. (2022). Padlet as a LMS platform in Arabic learning in higher education. Ingénierie des Systèmes d'Information, 27(4): 659–664. https://doi.org/10.18280/isi.270417

[9] Plummer, A.R., Beckman, M.E. (2016). Sharing speech synthesis software for research and education within low-tech and low-resource communities. In INTERSPEECH San Francisco, USA, pp. 1618–1622. https://doi.org/10.21437/Interspeech.2016-1540

[10] Li, X., Cen, Z., Liu, X., Zheng, Z. (2016). Online to offline teaching model in optics education: Resource sharing course and flipped class. In Optics Education and Outreach IV, 9946: 251–258. https://doi.org/10.1117/12.2237823

[11] Gao, Y. (2019). Educational resource information sharing algorithm based on big data association mining and quasi-linear regression analysis. International Journal of Continuing Engineering Education and Life Long Learning, 29(4): 336–348. https://doi.org/10.1504/IJCEELL.2019.102771

[12] Barbalios, N., Ioannidou, I., Tzionas, P., Paraskeuopoulos, S. (2013). A model supported interactive virtual environment for natural resource sharing in environmental education. Computers & Education, 62: 231–248. https://doi.org/10.1016/j.compedu.2012.10.029

[13] Mao, L. (2022). Resource sharing method of basic computer education based on mixed gaussian model. Mobile Information Systems, 2022: 6325329. https://doi.org/10.1155/2022/6325329

[14] Qiu, Z., Xiao, P., Nguyen, O. (2022). Construction of data resource sharing platform in college students' ideological and political education based on deep learning. Wireless Communications and Mobile Computing, 2022: 2905887. https://doi.org/10.1155/2022/2905887

[15] Habelko, O., Bozhko, N., Gavrysh, I., Khltobina, O., Necheporuk, Y. (2022). Characteristics of the influence of digital technologies on the system of learning a foreign language. Ingénierie des Systèmes d'Information, 27(5): 835–841. https://doi.org/10.18280/isi.270518

[16] Zhao, F. (2022). A resource sharing system for music education using the entropy technology. Mobile Information Systems, 2022: 3382742. https://doi.org/10.1155/2022/3382742

[17] Yuan, X. (2022). Network education resource information sharing system based on data mining. Mathematical Problems in Engineering, 2022: 4080049. https://doi.org/10.1155/2022/4080049

[18] Yu, X., Jiang, L. (2022). Design of cross language education resource sharing platform based on Hadoop framework. Multimedia Technology and Enhanced Learning, pp. 168–182. https://doi.org/10.1007/978-3-031-18123-8_13

[19] Wang, J. (2022). Resource cache sharing system of education information center network based on internet of things. Mobile Information Systems, 2022: 4947586. https://doi.org/10.1155/2022/4947586

[20] Zhu, Y., Dang, J., Wang, Y., Yong, J. (2021). Research on blockchain in digital education resource sharing in colleges and universities. In 2021 IEEE International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Fuzhou, China, pp. 570–577. https://doi.org/10.1109/CEI52496.2021.9574479

[21] Li, C.Y., Zhao, Q., Herencsar, N., Srivastava, G. (2021). The design of mobile distance online education resource sharing from the perspective of man-machine cooperation. Mobile Networks and Applications, 26(5): 2141–2152. https://doi.org/10.1007/s11036-021-01770-0

7 Authors

Bing Dai, female, associate professor. She received master degree in Vocational and technical Education from Hebei Normal University. She has more than 20 years' experience in teaching, she worked as a lecturer in Shijiazhuang Railway Transportation School from 2003 to 2016; since 2016, she has been working in Hebei Vocational College of Rail Transportation, and now she is the director of teaching and Research Office of Accounting Specialty. Email: daibing0416@163.com

Xiaoguang An, graduated from Hebei Normal University with a master's degree in education. Now she is working in Hebei Railway Transportation Vocational and Technical College. Her research interests include vocational education, photogrammetry and remote sensing. Email: anlistone@163.com

Article submitted 2023-01-28. Resubmitted 2023-03-03. Final acceptance 2023-03-03. Final version published as submitted by the authors.