Real-time Sharing Method of English Education and Teaching Resources Based on Blockchain Technology

Yingchun Fan[1*]

[1]Lecturer, Foundation college, Xi'an Urban Architectural College, Xi'an, China. Email: yingchun_fan1982@163.com

Abstract: The rapid development of information technology and the widespread use of the Internet have made sharing digital educational resources a crucial trend in the education sector. However, challenges such as dispersed storage and inadequate protection of intellectual property rights hinder efficient resource sharing. Blockchain technology offers a decentralized and secure solution to these challenges. This paper explores real-time sharing methods for English education and teaching resources based on blockchain technology. By designing secure sharing models and algorithms and constructing digital education resource sharing platforms, significant contributions have been made to address the challenges faced in resource sharing. The experimental analysis demonstrates the effectiveness of the proposed method, showing higher efficiency and security compared to traditional methods. Moreover, under the Windows 10 system, our method exhibits excellent performance, particularly in scenarios with numerous user attributes. This indicates its potential for widespread adoption in educational settings.

Keywords: Blockchain Technology, Digital Education Resource Sharing, Real-Time Sharing Method, English Education , Teaching Resources.

Introduction

With the rapid development of information technology and the popularization of the Internet, the sharing of digital educational resources has become an important trend in the field of education. Sharing educational resources not only helps to improve the efficiency and quality of education and teaching but also promotes educational innovation and academic exchange. However, the current sharing of educational resources still faces a series of challenges and obstacles, such as dispersed storage of resources and inadequate protection of intellectual property rights. In order to address these issues, scholars have begun to explore new sharing models and technological means. Among them, blockchain technology, as a decentralized and secure distributed ledger technology, has brought new possibilities for the sharing of educational resources [1]. This paper aims to study real-time sharing methods of English education and teaching resources based on blockchain technology. By designing secure and trustworthy sharing models and algorithms, constructing digital education resource sharing platforms, it aims to provide theoretical support and practical guidance for the digital transformation and innovative development of the education sector.

With the vigorous development of the big data industry, the sharing of educational resources has become an important trend in the informatization and digitization construction of universities and colleges. Sharing educational resources not only promotes educational innovation but also fully taps into the research value of universities and colleges, enhancing the quality of education. However, there are still some problems with the current resource sharing [2]. Firstly, educational resources are stored in databases scattered across various units of universities and colleges, leading to narrow resource utilization. Secondly, existing sharing methods lack effective records and rights confirmation for the flow and reuse of resources, which easily leads to intellectual property infringement and copyright disputes. In this context, the emergence of blockchain technology provides new ideas and approaches to solving these problems.

Blockchain technology is considered the next generation disruptive innovation technology, characterized by decentralization, trustlessness, tamper resistance, and transparency. Applying blockchain technology to the field of educational resource sharing can build a distributed database, achieve trustworthy traceability of resource sharing, and ensure data security, thereby promoting the full circulation and utilization of educational resources. This not only helps to eliminate information barriers between universities and colleges, promote resource cooperation, but also effectively protects intellectual property rights, enhancing the enthusiasm and efficiency of

resource sharing. Therefore, researching real-time sharing methods of English education and teaching resources based on blockchain technology is of great theoretical and practical significance.

This study will adopt a comprehensive approach, first analyzing the demand for sharing digital educational resources to understand the current problems and challenges. Secondly, it will design a secure sharing model for digital educational resources based on blockchain and access control, combining fine-grained access control based on attribute encryption to address privacy and security issues in resource sharing. At the same time, it proposes a CP-ABE algorithm that supports third-party pre-decryption to reduce the computational pressure on users and blockchain nodes. Finally, the study will build a digital education resource sharing platform in a modular manner, develop smart contracts, and deploy them on the blockchain network to achieve the orderly and secure circulation of resource data.

This study will provide important theoretical and methodological support for the research and practice of real-time sharing methods of English education and teaching resources. By designing a secure sharing model based on blockchain technology and a CP-ABE algorithm that supports pre-decryption, it solves the security and efficiency problems of traditional sharing methods, providing new solutions for the effective sharing and utilization of educational resources. In addition, the constructed digital education resource sharing platform has certain practicality and promotional value, which is of positive significance for promoting educational informatization and digitization construction.

Related Work

Overview of Blockchain

Blockchain technology is a distributed ledger system where data blocks are linked together in chronological order to create a chain. As illustrated in Figure 1, each block consists of two parts: the block header and the block body. The header contains a hash value that links the block to the previous one, a nonce (used for the proof-of-work mechanism), a timestamp, and the Merkle tree root, which allows for efficient summarization and validation of all transactions within the block. The block body holds the details of each individual transaction [3]. Key features of blockchain include immutability, decentralization, security, transparency, and privacy.

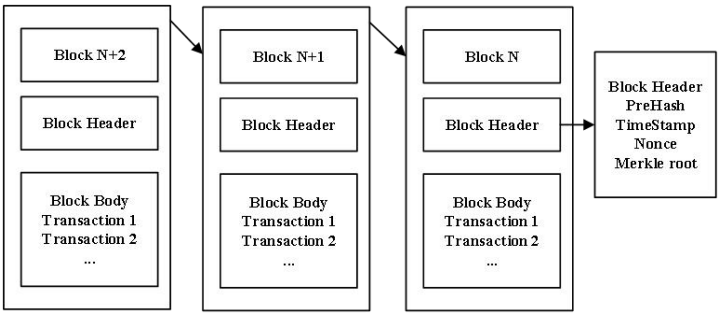

Figure 1. Blockchain Infrastructure Diagram

A blockchain system consists of multiple nodes, each capable of querying information and storing data, thus achieving decentralization. Decentralization means that the entire system does not rely on central servers, and the operation of any node does not affect the operation of the entire blockchain [4]. The openness of blockchain is reflected in the openness of its technology, allowing others to develop and innovate based on its functions. Its security comes from the encryption and consensus mechanisms within the blockchain, making data difficult to tamper with or modify, thereby protecting the security and credibility of the system [5].

Applications of Blockchain

Initially, blockchain technology was applied to solve issues in the circulation of Bitcoin. Over time, blockchain has gradually been applied in various fields such as financial market transactions, the Internet of Things and logistics, public services, insurance, and increasingly in higher education, becoming an important technological means to promote educational informatization and resource sharing.

In financial market transactions, blockchain platforms have deeply integrated with supply chain finance, electronic payment services, asset securitization, etc., improving the transparency and security of transactions [6]. This characteristic can also extend to the field of higher education, providing a more secure and transparent platform for sharing educational resources.

The application of blockchain technology in higher education mainly includes the construction of disciplinary curriculum systems, the construction of teaching information systems, and the exchange and mutual recognition of credits and courses between higher education institutions in different regions. For example, by building a blockchain platform, different universities can share course resources, teaching information, and academic achievements, promoting the interoperability and sharing of educational resources [7]. At the same time, blockchain technology can also be used to build student learning records and course certification systems, improving the credibility and traceability of student learning outcomes.

The Necessity and Feasibility of Blockchain Technology in the Sharing of Higher Education Resources

With the popularization and development of higher education online, resource sharing has become one of the important ways to solve the imbalance of educational resources and improve educational equity [8]. Meanwhile, the construction of online educational resources has also provided a broader platform for sharing higher education resources.

Blockchain technology can build functions such as smart contracts to achieve automated management and transactions of educational resources, improving resource utilization efficiency. Finally, the decentralized nature and security guarantee of blockchain technology can effectively prevent information leakage and infringement issues during the sharing of educational resources, promoting widespread sharing and utilization of educational resources.

In conclusion, blockchain technology has significant significance and application prospects in the sharing of higher education resources, providing important support for the digital transformation and innovative development of the education sector.

Design of Real-Time Sharing Method for English Education

An Teaching Resources Based on Blockchain Technology

Model of English Education Resource Sharing System Based on Blockchain Technology

Entities

The model of the English education resource sharing system based on blockchain technology involves six entities, including the Authorization Authority (AA), English Education Resource Owner (ER_Owner), English Education Resource Data User (ER_User), Third-party Pre-decryption, Decentralized Storage (IPFS), and Blockchain. The Authorization Authority (AA) is managed by blockchain network nodes, responsible for generating attribute keys and third-party pre-decryption keys, as well as encrypting education resource-related data [9]. The English Education Resource Owner is usually the creator of educational resources, responsible for encrypting education resource files and uploading them to the IPFS decentralized storage system, as well as setting access policies on the blockchain. The English Education Resource Data User is the learner of educational resources, who can obtain relevant information about educational resources and decrypt the target file after satisfying the access policy [10], [11]. To alleviate the computational pressure on the blockchain, the Third-party Pre-decryption participates in the first-stage decryption operation and hands over the intermediate ciphertext data to the English Education Resource Data User for final decryption. English Education Resource Data is stored in the decentralized IPFS InterPlanetary File System in encrypted form and returns address hash data. The blockchain is responsible for storing critical information, including records of user requests for attribute keys and English education resource sharing records.

System Framework

As shown in Figure 2, the system framework covers the data resource layer, business layer, smart contract layer, and data storage layer. In the data resource layer, there are basic user attribute data, English education resource information, private customized access policies, global attribute collections, and public and private keys to

ensure data security [12]. The business layer includes modules for system initialization, user login, resource creator publishing educational resources, learner access request, and third-party pre-decryption. The smart contract layer is responsible for handling transactions related to the business layer, such as user registration transactions, generation of user attribute key transactions, English education resource data on-chain transactions, and English education resource sharing record on-chain transactions. These smart contracts can be written in various languages, and the compiled code will be packaged and deployed on various organizational nodes. The data storage layer includes English education resource files encrypted and stored in IPFS, business object's current state stored in the world state, and the process of creating, modifying, and deleting business objects recorded on the blockchain.

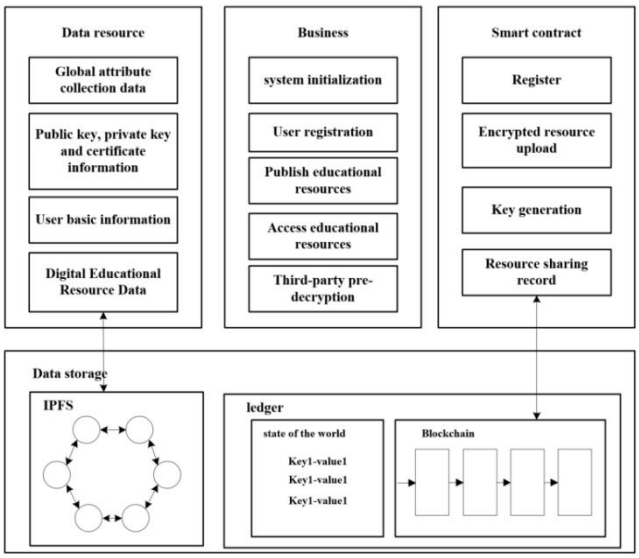

Figure 2. Framework

Digital Education Resource Data Access Control Model

As shown in Figure 3, the English education resource access control diagram includes the following three parts.

Platform User Registration: Users fill in personal information and send a registration request to the platform. The system generates a system public key (PK) and a master secret key (MSK) based on the input security parameter λ, and generates a key pair and certificate for the user[13]. The Authorization Authority (AA) converts the user's attribute set into a virtual attribute set and generates attribute keys (SK) and third-party pre-decryption keys (MidSK) for the user[14].

Publication of Educational Resource Data by Resource Creators: The ER_Owner creates educational resources and encrypts them using AES symmetric encryption. The encrypted educational resource files are uploaded to IPFS, generating an address hash (Address_Hash). The application platform connects to the blockchain network through an API interface and triggers smart contracts to encrypt the data, including KeyAES and Address_Hash. The encrypted data is uploaded to the blockchain, storing relevant information.

Access to Data by Resource Visitors: The ER_User applies to access educational resource files, triggering smart contracts to query and obtain ciphertext data (Ct) stored on the blockchain. The ciphertext is pre-decrypted by a third party. If the visitor's attributes satisfy the access policy, pre-decryption succeeds; otherwise, it fails[15]. The pre-decryption result is returned to the application platform, and a transaction request for digital educational resource sharing operation on-chain is submitted. After consensus, the sharing record is saved to the distributed ledger of the blockchain. If the attributes satisfy the access policy, the intermediate ciphertext is decrypted using the attribute key (SK) to obtain the file address (Address_Hash) and AES key, ultimately decrypting the educational resource file.

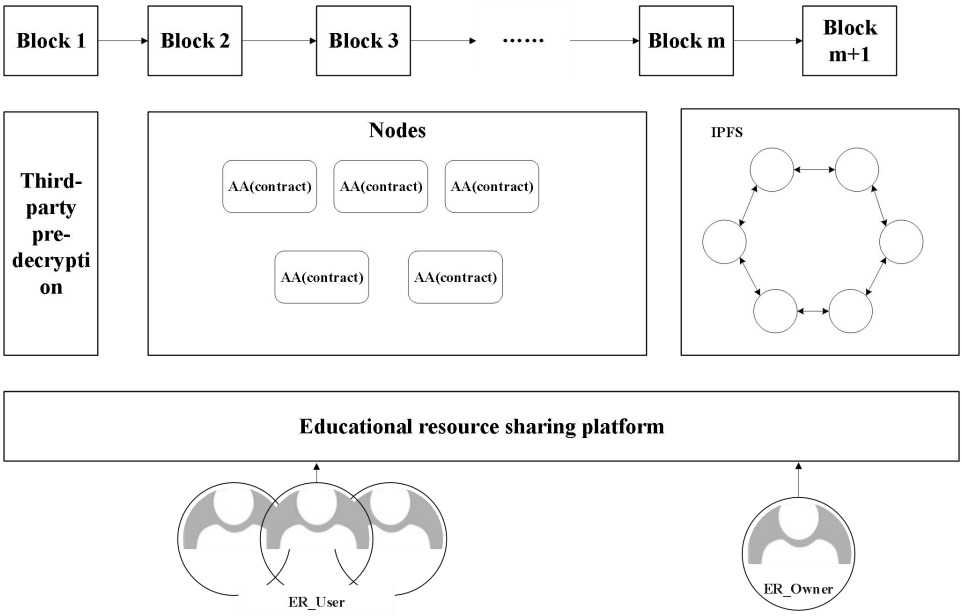

Figure 3. Access Control Model

CP-ABE Algorithm with Third-Party Pre-Decryption

CP-ABE (Ciphertext-Policy Attribute-Based Encryption) is an attribute-based encryption technique that allows data owners to define access policies, ensuring that only users who meet specific attribute requirements can decrypt and access data. To enhance security and prevent plaintext data leakage by third parties, the CP-ABE algorithm introduces a third-party pre-decryption mechanism, dividing the decryption process into two parts.

The core idea of the CP-ABE algorithm is to associate access policies with ciphertexts, allowing only users who satisfy the access policies to decrypt data [16]. To further protect user privacy, a third-party pre-decryption mechanism is introduced to replace full decryption, reducing the computational burden on users. The following are the main steps of the algorithm:

System Initialization

During system initialization, two multiplicative cyclic groups G1 and GT of prime order p generated by two generators g are selected, and a bilinear mapping e: G1 × G1 → GT is defined. Two random numbers and are chosen, generating the system public key (PK) and master secret key (MSK) as shown in formulas 1 and 2. Here, the function H is a hash function that maps attributes to elements in G1, making attribute transformation more convenient.

$$PK = (g, g^{\alpha}, g^{\beta}, e(g,g)^{\alpha}\beta) \tag{1}$$

$$MSK = \alpha \tag{2}$$

User Key and Third-Party Pre-Decryption Key Generation

The user key generation algorithm AttrPrvKeyGen takes user attributes (Attrs) as input, converts actual attributes into a virtual attribute set (Vir_Attrs), and then selects random numbers for each virtual attribute to generate user attribute key components and third-party pre-decryption keys. The user attribute key components are shown in formula 3, and the third-party pre-decryption keys are shown in formula 4.

$$SK_i = g^{Ti} \cdot e(g,g)^{\Sigma_i attr} \tag{3}$$

$$MidSK = g^{TSK} \tag{4}$$

Embedding Access Policies into Ciphertext Data

The encryption algorithm Encrypt first converts the access control policy into a specific form of access control tree, then calculates secret value fragments for leaf nodes, and finally generates ciphertext data. The generation of ciphertext components is shown in formula 5.

$$Ct = (m \cdot e(g,g)^{s}, \{g^{yi}, C_{yi} = e(g,g)^{s \cdot MD_j}\}) \tag{5}$$

Here, y is the set of leaf nodes, m is the data being encrypted, s is the secret value of the root node, and py(0) represents the value of the leaf node polynomial at x=0.

Third-Party Pre-Decryption Algorithm

The third-party pre-decryption algorithm performs pre-decryption in two steps: traversing the access policy tree and interpolating calculation for non-leaf nodes. Ultimately, the numerical value of the intermediate ciphertext (MidCt) is obtained.

$$Ct = (m \cdot e(g,g)^{s}, \{g^{yi}, C_{yi} = e(g,g)^{s \cdot MD_j}\}) \tag{6}$$

$$s_z = \frac{\prod_{y_i \in Y_z} C_{y_i}}{\prod_{y_i \in Y_z} e(g,g)^{\sum_{attr_k \in attr_{y_i}} MD_k}} \tag{7}$$

Final Decryption

Users perform the final decryption step by decrypting with the intermediate ciphertext (MidCt) [17] obtained through third-party pre-decryption to obtain the original data.

$$m = \frac{Ct_0}{e(MidCt, Ct1)} \tag{8}$$

These formulas and algorithm steps constitute the CP-ABE algorithm with third-party pre-decryption, ensuring data security and flexible access control.

Experimental and Analysis

Experimental Environment

We selected a pilot university in a certain region as the experimental subject and configured the experimental environment according to the parameters listed in Table 1. The configuration of the experimental environment includes aspects such as computer CPU, RAM, external hard disk memory, network card specifications, operating system, and kernel version [18]. We chose the Intel Xeon Processor (Skylake, IBRS) with good performance as the computer CPU, and configured 16GB of RAM and 500GB of external hard disk memory. In terms of networking, we used a gigabit network card, installed CentOS 7.2 or above as the operating system, and the kernel version was 4.15.2.17.x86_64.

Table 1 Parameter Settings

Serial Number	Project	Parameters
1	Computer CPU	2 194.848 MHz; Intel Xeon Processor (Skylake，IBRS)
2	RAM	16 GB
3	External Hard Drive Memory	500 GB
4	Network Card Specifications	nc. Virtio network device, Red Hat, Gigabit specification
5	Operating System	Centos 7.2 and above versions
6	Kernel Version	1160.15.2.el7.x86_64

After deploying the test environment, we installed the relevant software and set the operation versions according to the specific requirements of the experiment. Table 2 shows the software we installed and the corresponding operation version settings [19].

Table 2 Software Installation and Operation Version Settings in the Test Environment

Number	Software Version	Software Name
1	20.10.5	Docker
2	1.8	Java
3	1.15.1	Golang
4	2.0.0	JPBC
5	0.34.0	Tendermint
6	1.4.0	Hyperledger Fabric
7	8.0.10	Postman
8	5.4.1	Apache JMeter

Before setting up the blockchain network, it is necessary to configure the orderer organizations and peer organizations, including defining their names, domains, and the number of peer nodes in each organization. In addition, authentication of the identities of each authorization center organization is required. Subsequently, using the cryptogen tool, public-private key pairs and certificates for the participating organizations and nodes in this blockchain network are generated based on the configuration file, as shown in Figures 4 and 5. Once this process is completed, the identity files can be distributed to each organization.

Figure 4. Generating Identity Information Files

Figure 5. Generating the Genesis Block

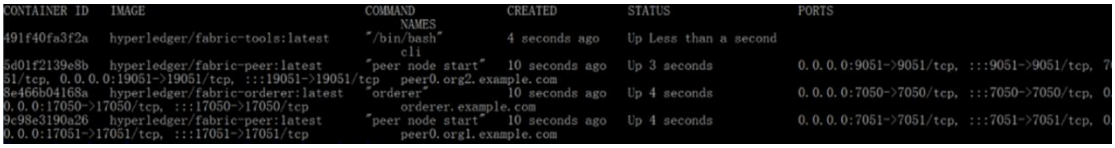

Figure 6. Creating node Docker Containers

Figure 7. Organizations Defining through Chaincode

Next is the generation of the genesis block. Each organization enters the blockchain network with their private keys and certificates, and each node is launched via Docker to join the network, creating node containers, as shown in Figure 6. This step ensures the initialization of the blockchain network and the joining of nodes, preparing for subsequent operations.

In this paper, we implement relevant interfaces using the Java language and compile smart contract code with annotations. Subsequently, as shown in Figure 7, the smart contract is deployed to the network channel, chaincode is installed on each node, and defined through chaincode. Finally, the chaincode is submitted to the channel to complete the setup of the blockchain environment. This process ensures the deployment of smart contracts and the execution of chaincode, providing a foundation for subsequent application development and data interaction..

Results Analysis

To meet the comparative requirements of the experiment, we introduced two traditional methods for education resource data sharing based on GT-DEMATEL (Traditional Method 1) and Asmuth-Bloom algorithm (Traditional Method 2), and compared them with the method proposed in this paper in terms of sharing education resource data in the IoT environment [20]. We selected the number of front-end concurrent request resource data that can be processed per second as the key indicator to evaluate sharing efficiency. The experimental results are shown in Figure 8.

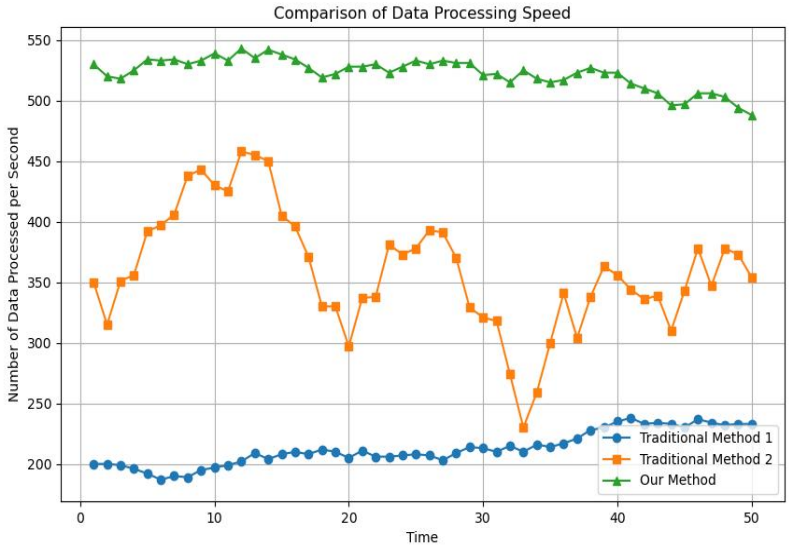

Figure 8. The Number of Front-End Concurrent Request Resource Data that can be Processed Per Second in the Share

From the experimental results in Figure 8, it can be seen that among the three methods, the method proposed in this paper achieves the highest number of resource data that can be processed per second when sharing education resource data. Traditional Method 1 also achieves a relatively high number of front-end concurrent request resource data per second, but its variability is unstable, leading to potential issues such as data interruption and loss during sharing transmission. The sharing transmission process of Traditional Method 2 is relatively stable, but compared with the method proposed in this paper, the number of front-end concurrent request resource data processed per second is lower. Based on the above analysis, we preliminarily conclude that the method proposed in this paper demonstrates relatively high efficiency in sharing education resource data in the IoT environment.

Building on the above experiments, we further set up different sharing transmission terminals and randomly introduced several malicious nodes and attack behaviors during the education resource data sharing transmission process. We detected the number of lost and abnormal data entries in different resource packets. The statistical results are shown in Table 3.

Table 3 Statistics on the Number of Lost and Abnormal Data Items During Transmission

Times	Our Method	Traditional Method 1	Traditional Method 2
1	0	15	2
2	0	21	5
3	0	9	6
4	0	7	7
5	0	14	5
6	0	23	3
7	0	32	4

From the experimental results shown in Table 3, it can be observed that among the three resource data sharing methods, only the method proposed in this paper can achieve zero lost and abnormal data entries during the resource data sharing transmission process. When using traditional methods for sharing education resource data, the resources experience varying degrees of packet loss when transmitted through IoT environment nodes due to external factors. In conclusion, the method proposed in this paper performs well in practical applications, not only improving the efficiency of resource data sharing but also enhancing the security of data transmission and effectively addressing issues such as packet loss during data sharing.

To analyze the optimal sharing solution, we will use three indicators: sharing latency, sharing throughput, and communication overhead. Below is the definition and comparison of these indicators: Sharing Latency: Refers to the time difference from sending a sharing request for online course educational resources to receiving feedback from the client-side node. In this experiment, a shorter sharing latency indicates a faster response speed of the resource sharing process. Sharing Throughput: Represents the maximum amount of shared resources completed per unit time without data loss in online course educational resources. A higher sharing throughput indicates that the system can process and transmit data more quickly. Communication Overhead: Refers to the total communication volume generated by all nodes to meet sharing demands when the client-side sends a sharing request. A lower communication overhead indicates that the system consumes fewer network resources during resource sharing.As show in table 4 and figure 9, let's compare the performance of the three methods based on these indicators:

Table 4. Performance of Three Methods Under Latency, Throughput, and Communication Overhead Indicators

Method	Sharing Latency (ms)	Sharing Throughput (bit/s)	Communication Overhead (KB)
Traditional Method 1	≤ 45	200 - 500	200 - 700
Traditional Method 2	≤ 40	350 - 500	150 - 450
Our Designed Method	≤ 25	500 - 700	85 - 200

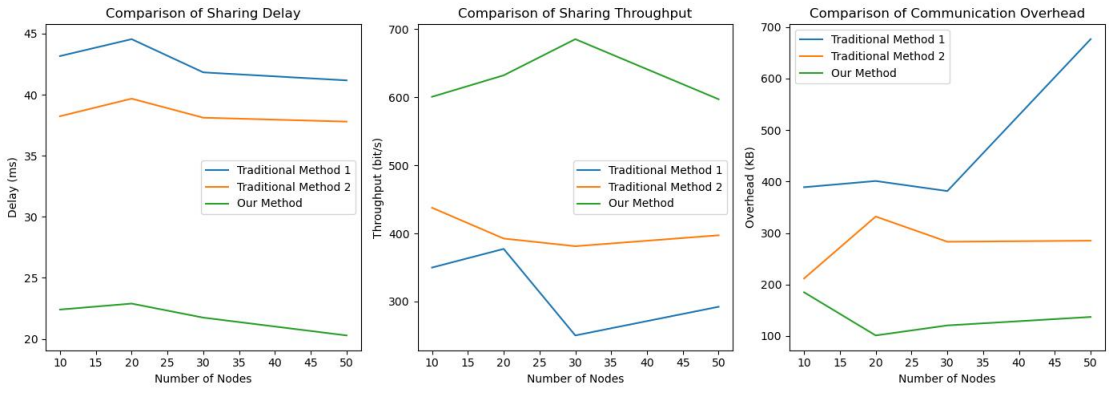

Figure 9. Comparison of Various Indicators

Based on the table above, the following conclusions can be drawn:In terms of sharing latency, our designed method performs the best, with the shortest sharing latency of no more than 25ms, which is much lower than the other two methods.In terms of sharing throughput, our designed method is also excellent, with the highest

throughput of 500 - 700 bit/s, while the throughput of the other two methods is slightly lower. In terms of communication overhead, our designed method also has an advantage, with the lowest communication overhead of no more than 200KB, far lower than the other two methods.

In conclusion, our designed method performs excellently in terms of sharing latency, sharing throughput, and communication overhead, making it one of the best sharing solutions.

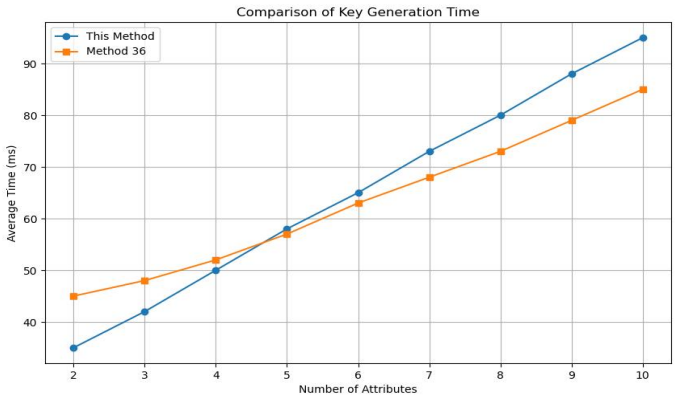

Figure 10 (a). Comparison of Key Generation Time

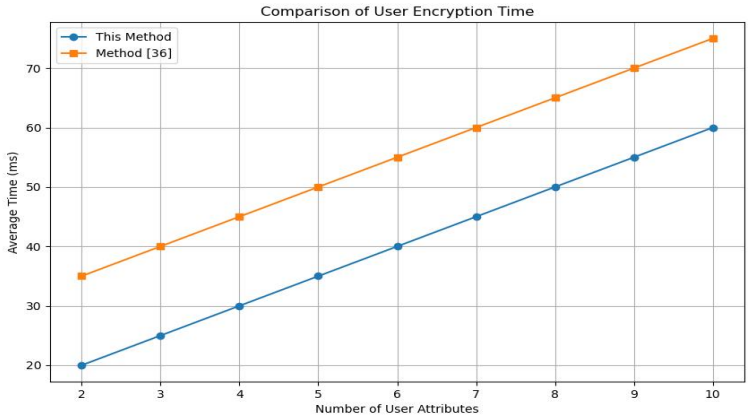

Figure 10 (b). Comparison of User Encryption Time

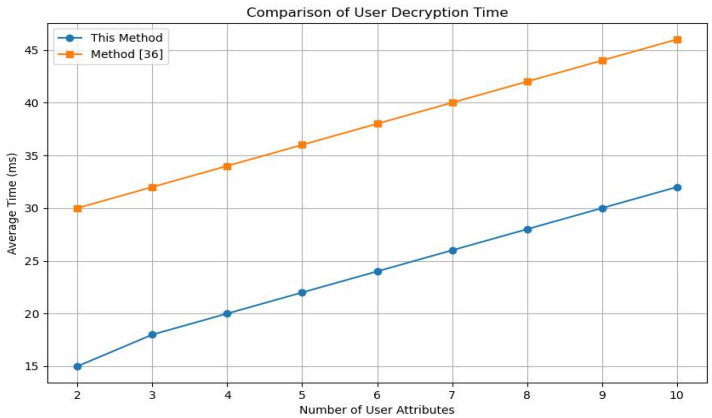

Figure 10 (c). Comparison of User Decryption Time

We present the performance comparison of different schemes under the Windows 10 system. As shown in Figure 10(a), from the key generation time comparison graph, it can be seen that the efficiency of key generation in our method is higher than that of method 36, especially when there are many user attributes, the difference is more significant. As shown in Figure 10(b), the comparison of access policy encryption time shows that our method requires less time for encryption compared to method. As shown in Figure 10(c), further observation of the comparison of user encryption time and user decryption time reveals that our method requires significantly less time for user encryption and decryption processes compared to Method [13], mainly due to the simplified process and optimized algorithms in our method. These results demonstrate that our method exhibits good performance under the Windows 10 system, especially when there are many user attributes. Compared to Method [13], our method can complete key generation, encryption, and decryption operations more quickly, thereby improving system response speed and efficiency.

Conclusion

Based on the research conducted, we conclude that blockchain technology presents significant opportunities for real-time sharing methods of English education and teaching resources. Traditional methods face challenges such as scattered resource storage and inadequate protection of intellectual property rights, which blockchain can effectively address. By implementing a secure sharing model based on blockchain technology and a CP-ABE algorithm with third-party pre-decryption, our proposed method ensures data security and flexible access control, enhancing the efficiency and security of resource sharing. Experimental results demonstrate that our method outperforms traditional approaches in terms of resource data processing speed and security. Compared to Traditional Method 1 and Traditional Method 2, our method achieves higher efficiency in sharing education resource data in IoT environments, with zero lost and abnormal data entries during transmission. Additionally, our method exhibits shorter sharing latency, higher sharing throughput, and lower communication overhead, making it a superior sharing solution. Furthermore, performance comparison under the Windows 10 system confirms the efficiency of our method, particularly in scenarios with many user attributes. The streamlined process and optimized algorithms contribute to faster key generation, encryption, and decryption operations, thereby enhancing system response speed and efficiency. In summary, our research provides theoretical and methodological support for real-time sharing methods of English education and teaching resources, offering practical solutions to improve resource sharing efficiency and security in educational settings.

Conflict of Interest

The authors declare no personal, professional, or financial conflict of interest regarding the publication of this work.

References

[1] Y. Hou, N. Wang, G. Mei, W. Xu, W. Shao, and Y. Liu, “Educational resource sharing platform based on blockchain network,” in *2019 Chinese Automation Congress (CAC)*, Nov. 2019, pp. 5491-5494. IEEE.

[2] J. Guo, C. Li, G. Zhang, Y. Sun, and R. Bie, “Blockchain-enabled digital rights management for multimedia resources of online education,” *Multimedia Tools and Applications*, vol. 79, pp. 9735-9755, 2020.

[3] S. Wang and C. Xu, “Intelligent sharing platform of agricultural online education resources based on blockchain technology,” in *International Conference on E-Learning, E-Education, and Online Training*, Cham: Springer Nature Switzerland, Jul. 2022, pp. 56-68.

[4] D. Shen, “Research on the sharing mode of educational information resources in colleges and universities based on the Blockchain and new energy,” *Energy Reports*, vol. 7, pp. 458-467, 2021.

[5] Brown, J.M.; Campbell, J.P.; Beers, A.; Chang, K.; Ostmo, S.; Chan, R.V.P.; Dy, J.; Erdogmus, D.; Ioannidis, S.; Kalpathy-Cramer, J.; et al., “Automated diagnosis of plus disease in retinopathy of prematurity using deep convolutional neural networks,” JAMA Ophthalmol., vol. 136, no. 7, pp. 803-810, 2018.

[6] Lin, S.R.; Ladas, J.G.; Bahadur, G.G.; Al-Hashimi, S.; Pineda, R., “A review of machine learning techniques for keratoconus detection and refractive surgery screening,” Semin. Ophthalmol., vol. 34, no. 4, pp. 317-326, 2019.

[7] Andrearczyk, V.; Müller, H., “Deep Multimodal Classification of Image Types in Biomedical Journal Figures,” in Proc. 9th Int. Conf. CLEF Assoc., CLEF 2018, Avignon, France, 10–14 Sept. 2018, pp. 3–14.

[8] D. Chen, H. Qiu, J. Zhu, and Q. Wang, "Research on blockchain-based interdomain security solutions," *Journal of Software*, vol. 31, no. 1, pp. 208-227, 2019.

[9] Bighash, E.Z.; Sadeghzadeh, S.M.; Ebrahimzadeh, E.; Blaabjerg, F., "Improving performance of LVRT capability in single-phase grid-tied PV inverters by a model-predictive controller," Int. J. Electr. Power Energy Syst., vol. 98, pp. 176-188, 2018.

[10] H. Xu, "Application and innovation of blockchain technology in performance management of public sector personnel under the background of governance modernization," *China Soft Science*, vol. 9, pp. 60-69, 2020.

[11] Elazab, O.S.; Debouza, M.; Hasanien, H.M.; Muyeen, S.M.; Al-Durra, A., "Salp swarm algorithm-based optimal control scheme for LVRT capability improvement of grid-connected photovoltaic power plants: Design and experimental validation," IET Renew. Power Gener., vol. 14, no. 6, pp. 591-599, 2020.

[12] L. Zhang, "Simulation research on the integration and sharing of public library resources under cloud computing," *Computer Simulation*, vol. 37, no. 5, pp. 416-419, 2020.

[13] Z. Zhang, "Data security sharing method based on CP-ABE and blockchain," *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 6-10, pp. 1-11, 2020, doi: 10.3233/JIFS-189318.

[14] Y. F. Hu and N. Z. Wu, "The authentication and conversion of online learning achievement: Obstacles, values and strategies," *Adult Education*, vol. 38, no. 08, pp. 27-32, 2018.

[15] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, pp. 461-466, 2016.

[16] G. Ilias, C. Cas, and K. B. Rasmussen, "When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 46-56, 2018.

[17] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, pp. 36-63, 2001.

[18] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, 2016.

[19] X. M. Yang, X. Li, H. Q. Wu, and K. Y. Zhao, "The application model and challenges of blockchain technology in education," *Modern Distance Education Research*, vol. 2, pp. 34-45, 2017.

[20] K. Croman et al., "On scaling decentralized blockchains: (A Position Paper)," in *International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg: Springer Berlin Heidelberg, Feb. 2016, pp. 106-125.