Research on Blockchain Based Data Sharing of Teaching Resources in Higher Vocational Mobile Education

Xiaoli Wang[1(✉)] and Mengxing Niu[2]

[1] Sanmenxia College of Social Administration, Sanmenxia 472000, China
16603989677@163.com
[2] Sanmenxia Polytechnic, Sanmenxia 472000, China

Abstract. The secure sharing of mobile education resources in vocational colleges refers to sharing student learning materials or other academic materials who have received vocational education in a secure and authorized manner to meet students' learning resource needs. Against the background of mobile internet and information-based society, vocational education needs to pay more attention to the sharing of educational resources to improve students' academic abilities and comprehensive qualities and enhance the quality of education and teaching. Secure sharing addresses the security issues of shared information. Therefore, a blockchain-based method for sharing data on vocational mobile education has been proposed. A compound chaotic password was constructed using the wavelet compound chaotic password matrix. Combined with blockchain technology, a secure model for sharing vocational mobile education teaching resource data was established. Experimental results showed that the computation time of this method was less than 150 s and can effectively increase operational efficiency. Furthermore, this system has low time and space overheads and high throughput, indicating that the proposed method can ensure secure sharing of educational resources.

Keywords: Blockchain Technology · Higher Vocational Mobile Education Teaching Resources · Data Sharing · Chaos Encryption · Digital Signature

1 Introduction

Vocational mobile education is one of the current development trends and future key directions, and has become a hot field of education development and teaching reform. Faced with the rapid development of vocational mobile education and the rapid updating of teaching resources, educational resource sharing has become an important solution [1, 2]. However, achieving the goal of sharing teaching resources in vocational mobile education still faces various challenges and difficulties. Due to the centralized operation and management method requiring the use of third-party platforms for data exchange, there is also a risk of data being copied or resold by third parties in the data sharing of vocational mobile education teaching resources. Education resources cannot be effectively protected, and the risk of leakage is relatively high. In order to effectively address

L. Yun et al. (Eds.): ADHIP 2023, LNICST 549, pp. 110–122, 2024.
https://doi.org/10.1007/978-3-031-50549-2_8

the above issues, relevant experts have conducted extensive research on the security sharing of teaching resources in vocational mobile education.

For example, Miao et al. [3] proposed a secure data sharing method for the Internet of Things based on joint deep reinforcement learning, using sensitive task decomposition and a layered asynchronous joint learning framework to achieve efficient and secure data sharing. At the same time, using deep reinforcement learning technology, select participants with sufficient computing power and high-quality data sets, and share local data models to achieve reliable data sharing, while protecting data privacy. Zhang et al. [4] proposed a cloud trust driven hierarchical sharing method for IoT information resources, which utilizes complementary judgment matrices and minimum non negative deviation values to obtain the optimal weight vector. At the same time, information security is considered and the information resource acquisition process is designed to ensure data reliability. By preprocessing the heterogeneous data collected by RFID devices and using trust based adaptive detection algorithms, evaluate the credibility of trust driven algorithms in limited resources and heterogeneous network environments, and achieve the sharing of data resources. Manogaran et al. [5] proposed a blockchain assisted secure data sharing model for the intelligent industry based on the Internet of Things, which manages the security of data collection and dissemination, including inbound and outbound. Identify bad data sequences through recursive learning techniques. Outbound security measures use blockchain information based on reputation and sequence differentiation for end-to-end authentication, in order to achieve resource information sharing.

Combining the above research methods, a blockchain based data sharing method for vocational mobile education teaching resources is proposed. In the wavelet transform space, the wavelet coefficients of plaintext information are encrypted by compound chaos, and the security model of educational resource data sharing is established by combining blockchain technology and hash function. The hash function is used to verify the data integrity, and the digital signature and hash value are uploaded to the blockchain for storage, so as to realize the safe sharing of teaching resource data of higher vocational mobile education. The experimental results show that this method completes the calculation in a relatively short time and effectively improves the system's operational efficiency. In addition, the proposed method has small time and space costs, high throughput, and can ensure the safe sharing of educational resources.

2 Safe Sharing Methods for Teaching Resources in Vocational Mobile Education

2.1 Information Resource Encryption

In order to effectively ensure the safe sharing of teaching resources in higher vocational mobile education, two one-dimensional chaotic systems are selected to establish a complex chaotic system. In order to improve the encryption performance of the chaotic system, the correlation coefficient and uniformity index are selected to establish a comprehensive objective function, and the adaptive chaos immune particle swarm optimization algorithm is introduced to optimize the control parameters in the system.

Logistic mapping is a one-dimensional discrete dynamical system, and the analytical equation corresponding to Logistic mapping is shown in formula (1):

$$z_{n+1} = \beta z(1 - z_n) \tag{1}$$

In the equation, z represents a chaotic variable; β represents chaotic parameters; n represents a constant.

After determining the control parameters, select corresponding time series for different initial values z_0. For different control parameters, the system exhibits different characteristics, and after continuous bifurcation operations, the system ultimately reaches a chaotic state.

The analytical equation corresponding to Cubic mapping is shown in formula (2):

$$z_{n+1} = xz_n^3 - yz_n \tag{2}$$

In the equation, x and y represent control parameters.

By establishing a complex chaotic system, information resources can be encrypted. Analyze the independence and convenience of chaotic systems, and effectively ensure the diversity and convenience of the initial particle swarm through chaotic initialization operations. The fitness value ω of different particles is calculated as follows:

$$\omega = \frac{\omega_{\min}}{(\omega_{\max} - \omega_{\min})} \tag{3}$$

where, $\omega_{\max}$ and $\omega_{\min}$ are the maximum and minimum fitness values respectively.

After obtaining the value of fitness, it is necessary to adaptively adjust the inertia weight coefficient in the evolution process to ensure that the convergence speed and convergence accuracy of the algorithm are effectively improved and find a better global optimal solution. Chaotic mutation operation can effectively screen out inert particles and remove them all, avoiding the algorithm from falling into local optima. The control parameter coordination optimization process ψ_1 is given through formula (4):

$$\psi_1 = D_{oef}\,\omega(x_1, y_1) + u_1(x) + u_2(x) \tag{4}$$

In the formula, D_{oef} represents the correlation coefficient; $u_1(x)$ and $u_2(x)$ represent different uniformity indicators; (x_1, y_1) represents the degree of concealment of ciphertext.

After completing the above operations, effectively combine it with wavelet composite chaotic encryption to encrypt teaching resource information [6–8]. The detailed operation steps are as follows:

The basic wavelet function $\varpi(n)$ in Fourier wavelet transform is transformed into a function cluster $\varpi_{e,\tau}(n)$ by scaling and translation:

$$\varpi_{e,\tau}(n) = \frac{\psi_1}{\sqrt{\phi}}\alpha\left(\frac{t - \alpha}{\phi}\right) \tag{5}$$

In the formula, ϕ represents the stretching parameter; α represents the translation parameter; t represents the operating cycle.

The Fourier wavelet transform satisfies the constraint condition I_ψ in formula (6):

$$I_\psi = \int_R \frac{|\varpi(n)|^2}{\omega} d\omega \tag{6}$$

where, $\varpi(n)$ represents the basic wavelet function; R represents a constant; d represents the wavelet coefficient.

Put function $s(t)$ in the two-dimensional real space into the wavelet transform space, and obtain the corresponding basic wavelet function through a series of operations to realize the wavelet transform. Combining the cryptography of wavelet transform and composite chaotic sequences to form a wavelet composite chaotic cryptosystem. Expand and optimize all system parameters to obtain 2 initial keys and 1 composite chaotic block key corresponding to the system. The corresponding calculation formula is:

$$\begin{cases} \partial_1 = \dfrac{\varpi_{e,\tau}(n)(c_1 + c_2) \cdot c_3}{s_{\min}} \\ \partial_2 = \dfrac{\varpi_{e,\tau}(n)(c_1 + c_2 + c_3)}{s_{\max}} \\ \partial_3 = \dfrac{(s_{\max} - s_{\min})}{\varpi_{e,\tau}(n)(c_1 + c_2 - c_3)} \end{cases} \tag{7}$$

In the formula, ∂_1 and ∂_2 represent different initial keys; ∂_3 represents a mixed chaotic block key; c_1. ∂_2 and c_3 represent different ciphertext information, respectively; $s_{\max}$ and $s_{\min}$ represent the maximum and minimum approximate entropy.

Two initial keys of the system are iteratively operated to obtain a brand new discrete chaotic sequence, and related operations such as displacement transformation are carried out to obtain a composite chaotic cryptographic sequence $Z_{(c)}$, as shown in formula (8):

$$Z_{(c)} = \partial_1 p(n - E_{m1}) I_{m1} \otimes \partial_2 p(n - E_{m2}) I_{m2} \tag{8}$$

where, p represents step function; E_{m1} and E_{m2} represent different time delays; I_{m1} and I_{m2} represent different composite parameters.

By using a block key to perform bandpass filtering on the composite chaotic cryptographic sequence, a composite chaotic encryption sequence with the same length as the wavelet transform sequence is obtained [9–11]. At the same time, binary or encryption operations are performed on it to obtain the ciphertext sequence $Z_{(ci)}$:

$$Z_{(ci)} = \partial_3 \left[p(n - E_{m1}) - p(n - E_{m2} - I_{m1}) \right] Z_{(c)} \otimes Z_{(swt)} \tag{9}$$

In the formula, $Z_{(swt)}$ represents a wavelet transform sequence.

After performing wavelet transform on plaintext sequence $Z_{(I)}$, continue to perform proportional transform on it to obtain wavelet transform sequence $Z_{(swt)}$ as shown in formula (10):

$$Z_{(swt)} = B_c \cdot \varpi(n) \tag{10}$$

In the equation, B_c represents the scaling factor.

By calculating the fitness value corresponding to the ciphertext sequence, determine whether the fitness value meets the set constraints, and if so, encrypt it; On the contrary, it is necessary to modify the control parameters of the composite chaotic system, re constrain it, and then encrypt the teaching resource information. Assuming completion, directly output the results to achieve encryption of teaching information resources for vocational mobile education. Otherwise, the fitness value corresponding to the ciphertext sequence needs to be recalculated.

2.2 Construction of a Security Sharing Model for Teaching Information Resources

Due to the random distribution of shared information in the network environment, the process of information sharing is more complex and cumbersome, which affects the security of information sharing. Blockchain has the characteristics of decentralization, tamper resistance, traceability, and high security, enabling efficient and secure sharing of data. Storing encrypted data on the blockchain can ensure the integrity and authenticity of the data, prevent data from being tampered with, and eliminate the intervention of intermediate institutions to achieve point-to-point data sharing. This not only improves the efficiency of data sharing, but also reduces risks in the data sharing process and enhances data security. In order to improve the security of information sharing, blockchain technology is introduced to construct a teaching information resource security sharing model [12–14].

The blockchain architecture is divided into five levels, namely application layer, contract layer, data layer, blockchain layer, and logical layer. The blockchain architecture is shown in Fig. 1, and each level is defined and its specific functions are as follows:

(1) Logic layer

It is mainly responsible for abstraction and analyzing various functions corresponding to intelligent cooperation, and providing users with simple and clear function calls. The work of related modules is mainly communicated by the Restful interface.

(2) Blockchain layer

This level is mainly responsible for completing related operations such as data sharing and permission interaction. Considering the needs of actual business scenarios, it is necessary to choose private chain as the blockchain network $P(x, y, z)$ of the original system, and the corresponding calculation formula is as follows:

$$P(x, y, z) = \{u, t, \beta, \delta\} \tag{11}$$

In the formula, u represents the blockchain unit; t represents the sampling period; β represents the incentive mechanism on the blockchain; δ represents the total number of public chains.

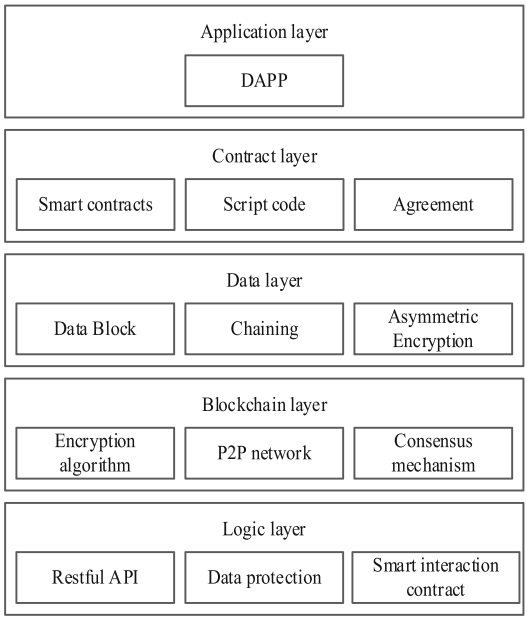


Fig. 1. Blockchain Architecture Diagram

This level also undertakes the task of defining content related to blockchain technology, such as block structure, digital signatures, information transmission, consensus mechanisms, etc. Information sharing involves multiple aspects of information data, and there are significant differences in information and different requirements for security. Through the processing of the blockchain layer, normalization processing of different information can be achieved [15, 16]. The normalization processing formula for shared information is:

$$Y_i = \frac{X_i - X_{\min}}{X_{\max} - X_{\min}} \tag{12}$$

In Eq. (12), X_i and Y_i respectively represent the shared information before and after normalization processing; $X_{\min}$ and $X_{\max}$ represent the minimum and maximum values of shared information, respectively.

(3) Data layer

The main purpose of the data layer is to achieve different types of data transactions, encapsulating the processed data into blocks, and then directly transmitting them to the corresponding blockchain database. The transaction order is composed of timestamp and hash values.

(4) Contract layer

In the model, it plays a logical control role. As different functions are coordinated by different contracts, corresponding contracts need to be constructed based on actual needs;

(5) Application layer

After receiving the requirements from the demand side, this level confirms and analyzes the shared information requirements, extracts corresponding shared information based on the requirements content, and integrates it.

In blockchain, each node needs to synchronize the entire chain information, as the storage capacity of each block data is limited. If the transaction iteration volume is large, it will affect the efficiency of consensus. In order to effectively improve resource utilization, it is necessary to store all critical information resources on the chain, determine the correlation between data on and off the chain, and establish a corresponding teaching information resource security sharing model $I_{(p)}$, as shown in formula (13):

$$I_{(p)} = Y_i\left\{t_1 \times Z_{(ci)} + t_2 \times Z_{(ci)}\right\} \times N_{(r)} \tag{13}$$

In the formula, t_1 and t_2 respectively represent different sampling stages; $N_{(r)}$ represents a random number generator.

The application layer also incorporates a data integrity verification mechanism. In the verification process, the hash function is used to verify the data integrity [17–19], and SHA-256 is used to obtain the corresponding digital signature; Upload all encrypted data to the private network, store it in the IPFS distributed file manager, and generate a blockchain hash value $H_{(a,b,c)}$, corresponding to the calculation formula:

$$YD = \left\{M_D, K_D, Z_{(ci)}, f_P\right\} \tag{14}$$

$$H_{(a,b,c)} = \frac{P(x, y, z) - N_{(r)} \times I_{(p)}}{Z_{(ci)}} \tag{15}$$

where, YD represents the meta Information set storing data; Formula (15) represents the process of storing data in IPFS to generate a blockchain contract hash value. K_D represents the keyword of the data; f_P is the unique access policy for encrypted data; M_D indicates the name of the data element.

Upload all digital signatures and generated hash values onto the blockchain. Assuming that the owner of teaching information resources agrees to share securely, the data requester will obtain the address corresponding to the data file, and at the same time expand the digital signature calculation through the hash function to compare the digital signature obtained by the calculation with the digital signature of the data owner, thus realizing the verification of data integrity [20–23]. The specific verification rules are as follows:

$$\begin{cases} \vartheta_i \geq \xi & \text{legal} \\ \vartheta_i < \xi & \text{Illegal} \end{cases} \tag{16}$$

In the formula, ϑ_i represents the digital signature of the i-th party requesting shared information; ξ represents the threshold for setting digital signatures for authentication.

In summary, complete the secure sharing of teaching information resources in vocational mobile education.

3 Experimental Analysis

In order to verify the effectiveness of the proposed blockchain based teaching resource data sharing method for vocational mobile education, the experiment used reference [3] on the blockchain based model for sharing cultural relics information resources (referred to as the "reference [3] method") and reference [4] on the decentralized ciphertext data security sharing method with anti-attribute tampering (referred to as the "reference [4] method") as comparative methods. The experiment was conducted in the Windows 10 system environment using IDEA programming software for simulation testing, and experimental analysis was conducted from the following aspects.

3.1 Result Analysis

The experiment uses system operating efficiency, operating expenses, and throughput as evaluation indicators to verify the security sharing performance of teaching information resources in vocational mobile education.

Operational efficiency refers to the time and computing resources required for a data sharing method to actually run. For the data sharing method of mobile education teaching resources, the operating efficiency directly affects the user experience and the response speed of the system. If the operation efficiency of the data sharing method is low, the delay of data transmission and processing may be increased, which will affect the real-time performance of teaching resources and user experience.

The operating overhead includes resources such as hardware devices, software platforms and network bandwidth required by the data sharing method. The data sharing method of mobile education teaching resources needs to take into account the computing power, storage capacity and network connection stability of mobile devices. The data sharing method with low operating cost can improve the utilization efficiency of resources, reduce the cost and adapt to the environment requirements of various mobile devices.

Throughput refers to the volume of requests or data traffic that a data sharing method can handle. For the data sharing method of mobile education teaching resources, high throughput means that more users can access and share resources at the same time, and improve the scalability and capacity of the system. Therefore, the data sharing method with higher throughput can meet the needs of large-scale users and provide stable and efficient teaching resource sharing service.

Operation efficiency, operation cost and throughput are the key indicators to evaluate the performance of mobile education teaching resource data sharing method, which directly affect the practical application and user experience of the system.

(1) System operational efficiency testing

System operational efficiency is one of the indicators for evaluating system operational performance. Usually refers to the amount of tasks processed by the system under a specific workload. The higher the operational efficiency, the greater the workload and task volume that the system can handle, and the better the system performance. A higher value indicates that the system is processing more tasks. If the operational efficiency of the system decreases, it indicates potential faults or other safety issues in the system. The

experiment mainly measures the operational efficiency of different methods by calculating time. The experimental results of the operational efficiency of different methods are shown in Fig. 2.

From Fig. 2, it can be seen that in the initial stage of the experiment, the calculation time of different methods is less than 100 s. However, as the sample continues to increase, the calculation time of the methods in reference [3] and [4] significantly increases, especially when the sample size is large, the maximum calculation time exceeds 150 s. The overall calculation time of the proposed method is less than 150 s and is less affected by the number of samples. Through comparison, it can be seen that the proposed method has the shortest calculation time, fully demonstrating its advantages in improving system operation efficiency.

(2) System running cost testing

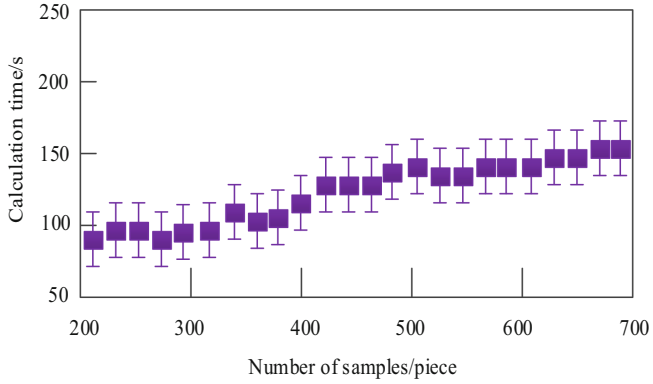
Running cost refers to the cost of resources and time consumed by a computer when executing a specific program. This typically includes system hardware resource consumption (such as CPU usage, memory consumption, etc.) and time consumption (such as response time and processing time, etc.). The lower the running cost, the better the system performance. A larger value indicates that the system consumes more resources and time, resulting in higher operating costs. Meanwhile, if the operating cost of the system increases, it indicates that the system faces more security risks, as some security measures can increase the operating cost of the system. The experimental results of comparing overhead in time and space using different methods are shown in Fig. 3.

Further analysis of (a) in Fig. 3 shows that as the amount of shared data during system operation increases, there is a significant difference in the time cost of the system. The overall time cost of the proposed method system is less than 5 s. The system time cost of the methods in reference [3] and [4] is higher than that of the proposed methods. This indicates that the proposed method can process data quickly and efficiently in data sharing scenarios, thereby improving the system's running speed and service quality. Analyzing Fig. 3 (b), it can be seen that under the same amount of data sharing, the spatial overhead of the proposed method system is smaller than the methods in reference [3] and [4]. The smaller the spatial overhead of a data sharing system, the higher the likelihood that the system can support larger scale data sharing in the future. It can be seen from the comparison that the system operation of the proposed method provides less space for data sharing services, which can effectively reduce overhead and improve the system operation speed.

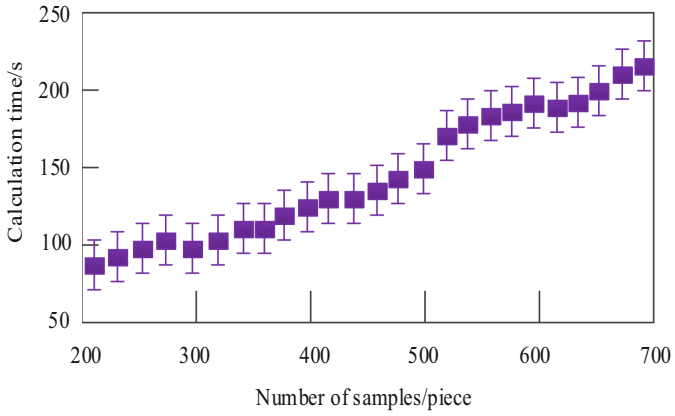
In summary, the proposed method has excellent performance in data sharing and can provide efficient data sharing services for the system.

(3) Throughput testing

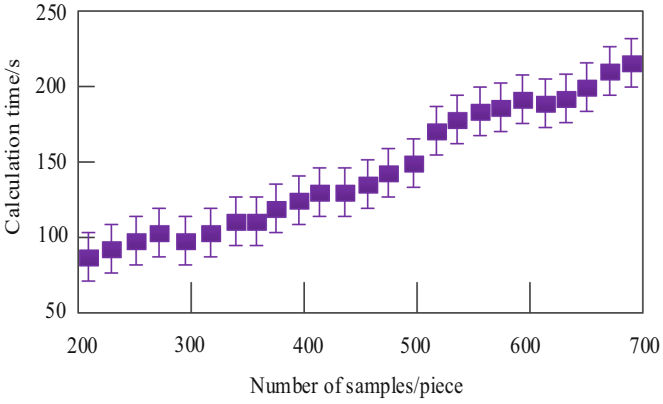
Throughput is an indicator that measures the number of tasks a system can complete per unit of time. Usually refers to the amount of data that a computer can process per unit of time. The higher the throughput, the stronger the system's concurrency and efficiency. The larger the value, the more concurrent tasks the system can handle. It also reflects the efficiency of information sharing. The higher the value, the higher the efficiency of information sharing. If shared resources are attacked by hackers or abused by some



(a) Proposed method

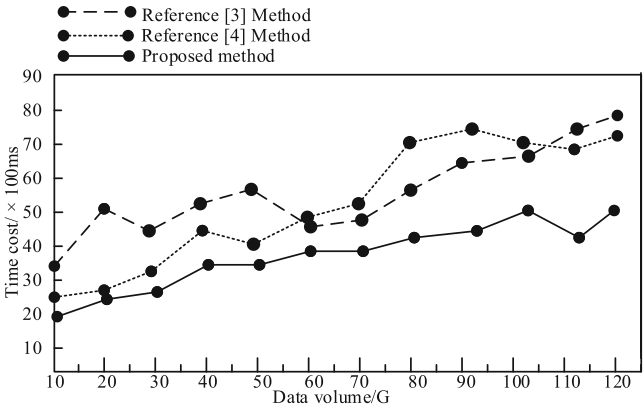


(b) Reference [3] Method

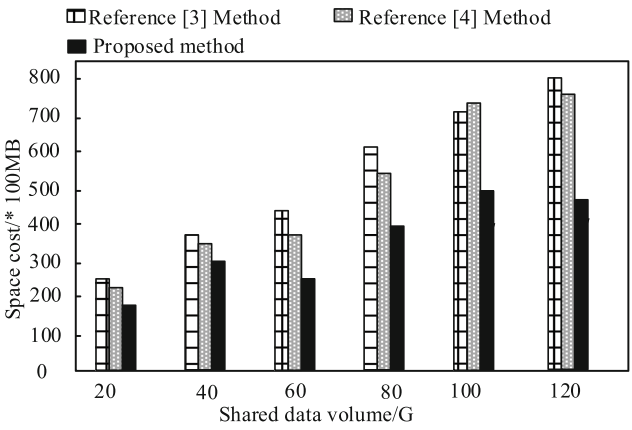


(c) Reference [4] Method

Fig. 2. Comparison of experimental results on operational efficiency of different methods



(a) System Time Cost Comparison



(b) System Space Cost Comparison

Fig. 3. Comparison of operating costs of data sharing systems

malicious users, it can lead to a decrease in the system's throughput. The experimental results of information sharing throughput using different methods are shown in Fig. 4:

From the experimental results in Fig. 4, it can be seen that the throughput of the proposed method has been continuously increasing in a straight line, with a clear upward trend. However, the throughput of the methods in reference [3] and [4] is significantly lower than that of the proposed method. This shows that the proposed method can more effectively utilize system resources and achieve more efficient data sharing, indicating that the teaching information sharing efficiency of the proposed method is high and can effectively reduce hacker attacks, Ensure the secure sharing of teaching information resources.

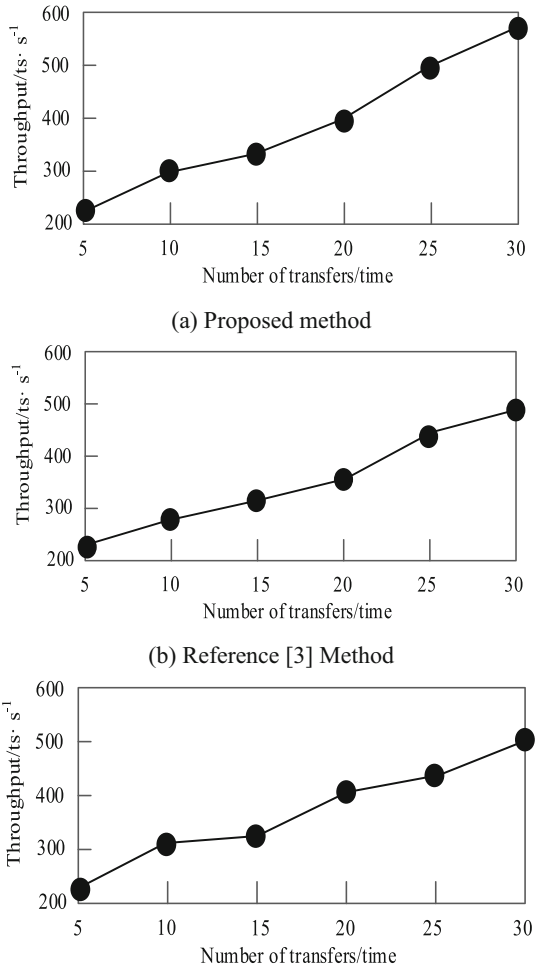


Fig. 4. Comparison of experimental results of information sharing throughput using different methods

4 Conclusion

In order to ensure the safe sharing of teaching resource data of mobile education in higher vocational colleges, a method based on blockchain technology is proposed. In this study, a method of data security sharing of vocational mobile education teaching resources based on blockchain technology is designed. Chaotic sequences are used to initialize the fitness values of different particles, which can increase the randomness and security of cryptosystems. A more complex and secure cryptosystem is constructed by combining wavelet transform with chaotic cryptosystem. Wavelet transform can improve the data concealment and anti-interference ability, while chaotic cryptosystem can increase the

randomness and unpredictability of cryptography. By combining the two, stronger data encryption and decryption capabilities can be achieved. Blockchain technology can provide a reliable data verification mechanism, by hashing the data and recording the hash value on the blockchain, you can verify whether the data has been tampered with. At the same time, blockchain can also be used to generate and verify digital signatures, ensuring the authenticity of data and trusted sources.

References

1. Xu, M., Ma, S., Wang, G.: Differential game model of information sharing among supply chain finance based on blockchain technology. Sustainability **14**(12), 7139 (2022)
2. Singh, C.E.J., Sunitha, C.A.: Chaotic and Paillier secure image data sharing based on blockchain and cloud security. Expert Syst. Appl. **198**, 116874 (2022)
3. Miao, Q., Lin, H., Wang, X., et al.: Federated deep reinforcement learning based secure data sharing for internet of things. Comput. Netw. **197**, 108327 (2021)
4. Zhang, J.: Cloud trust-driven hierarchical sharing method of internet of things information resources. Complexity **2021**, 1–11 (2021)
5. Manogaran, G., Alazab, M., Shakeel, P.M., et al.: Blockchain assisted secure data sharing model for internet of things based smart industries. IEEE Trans. Reliab. **71**(1), 348–358 (2021)
6. Liu, Y., Ko, Y.C.: Image processing method based on chaotic encryption and wavelet transform for planar design. Adv. Math. Phys. **2021**, 1–12 (2021)
7. Welba, C., et al.: Josephson junction model: FPGA implementation and chaos-based encryption of sEMG signal through image encryption technique. Complexity **2022**, 1–14 (2022). https://doi.org/10.1155/2022/4510236
8. Lingamallu, N.S., Veeramani, V.: Secure and covert communication using steganography by wavelet transform. Optik **242**, 167167 (2021)
9. Liu, L., Meng, L., Peng, Y., et al.: A data hiding scheme based on U-Net and wavelet transform. Knowl.-Based Syst. **223**, 107022 (2021)
10. Deb, N., Elashiri, M.A., Veeramakali, T., Rahmani, A.W., Degadwala, S.: A metaheuristic approach for encrypting blockchain data attributes using ciphertext policy technique. Math. Probl. Eng. **2022**, 1–10 (2022). https://doi.org/10.1155/2022/7579961
11. Rahman, M.S., Khalil, I., Moustafa, N., et al.: A blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted industrial internet of things systems. IEEE Trans. Industr. Inf. **18**(7), 5007–5017 (2021)
12. Sifah, E.B., Xia, Q., Agyekum, K.O.B.O., et al.: A blockchain approach to ensuring provenance to outsourced cloud data in a sharing ecosystem. IEEE Syst. J. **16**(1), 1673–1684 (2021)
13. Wu, C., Ke, L., Du, Y.: Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain. Inf. Sci. **548**, 438–449 (2021)
14. Miao, W.H., Wang, J.X., Zheng, Z.H.: Identity authentication scheme based on blockchain and multi factor combination. Comput. Simul. **39**(5), 402–408 (2022)
15. Tang, G., Zhang, Z.: Two-party signing for ISO/IEC digital signature standards. Comput. J. **66**(5), 1111–1125 (2022). https://doi.org/10.1093/comjnl/bxac001