Reliability Detection Method of Online Education Resource Sharing Based on Blockchain

Feng Wang(✉)

Jiujiang University, Jiujiang 332005, China
wangfengl7172021@163.com

Abstract. In order to reduce the error of online education resource sharing reliability detection, a block chain based online education resource sharing reliability detection method is designed. This paper first analyzes the status of online education resource sharing, then defines the reliability of information resource sharing system, and finally establishes the reliability detection model of online education resource sharing to realize the reliability detection of education resource sharing. The experimental results show that the proposed method has smaller detection error and higher sharing security than traditional methods.

Keywords: Blockchain · Online education · Resource sharing · Reliability

1 Introduction

With the development and popularization of computer network technology and multimedia technology, network education, as a form of education, has developed rapidly in higher vocational colleges. It breaks through the limitation of time and space in the traditional education process and realizes the sharing of teaching resources in a wider range. At present, many countries attach great importance to the construction of online teaching resources, such as the "educational technology action plan" and "American Education Action Plan" of the United States, the CTI plan of the United Kingdom, the school networking plan of France, the education network plan of Australia, the "education revolution" of South Korea, the cross century plan of Singapore and the school networking experiment of Japan. However, there are many problems in the security of campus network, so the security of network teaching resources can not be effectively guaranteed, which also restricts the construction and sharing of network teaching resources in Higher Vocational Colleges to a certain extent.

Any science and technology is a "double-edged sword". Information resource sharing system has its own vulnerability. System security and reliability is the most important and basic requirement, and also the premise for the existence and development of information resource sharing system. How to improve the reliability of the system and prevent the unreliable factors is one of the keys of the system design. Therefore, the reliability detection method of online education resource sharing is studied. Traditional methods generally use data mining to share online education

S. Wang et al. (Eds.): IoTCare 2021, LNICST 414, pp. 399–416, 2022.
https://doi.org/10.1007/978-3-030-94185-7_27

resources, but the reliability of sharing is poor because of the huge amount of online education resources data and the huge types of resources and data involved.

Blockchain is a kind of database with hash verification function. Block is the data block. It combines the data blocks into a chain structure according to the time sequence, and uses the cryptography algorithm to maintain the reliability of the database collectively in the way of Distributed Accounting. All data blocks are connected in chronological order to form a blockchain. Based on the characteristics of blockchain technology, this paper designs an online education resource sharing reliability detection method based on blockchain. On the basis of clarifying the status of online education resource sharing, the reliability of education resource information sharing system is defined. Based on this, the reliability testing model of online education resource sharing is established to realize the reliability testing of education resource sharing.

2 Online Education Resource Sharing

In today's global education information environment, the construction of information-based education environment is an important part of education modernization. In the current higher vocational colleges, network teaching resources have the advantages of timeliness of information and resource transmission, students' autonomy in learning, interaction between teaching and learning, and sharing of teaching resources. All schools attach great importance to it, and build their own network teaching resource system to reform the traditional teaching and management mode, and build a network learning platform for students' autonomous learning and collaborative learning [1]. At present, in the general campus network, network teaching resource system is mainly divided into four layers: basic layer, resource management layer, application layer and user layer. Among them, the basic layer refers to the basic platform of campus network operation, and CERNET and Chinanet are the main connecting networks of higher vocational colleges; The resource management layer is generally composed of database server and resource server group, such as IP server, e-mail server and streaming media server; The application layer is mainly composed of web server and related applications; The user layer is mainly composed of teachers and students in the campus network. The system structure of the four layer network teaching resource management system has laid a solid foundation for the sharing of teaching resources in campus network, but there are many security problems in the actual use of network teaching resources, which will restrict the construction and development of network teaching resource system in higher vocational colleges. Therefore, it is necessary to analyze these security problems and find a reasonable method of sharing network teaching resources.

3 Reliability Definition of Information Resource Sharing System

In the actual operation, information resource sharing system may face various errors or exceptions, which can be attributed to some external factors (such as artificial error, network or hardware abnormality). An information resource sharing system should

ensure that there is a pre-defined framework or mechanism to handle errors or recover from errors. Therefore, reliability becomes an important index of the performance of distributed information resource sharing system.

Reliability refers to the probability that the system operates normally and correctly performs the required functions under the specified operating environment and within the specified time period. The strong reliability of the system means that when the external environment or internal state changes or abnormally, the system can still complete its preset function, without stopping the system running or crashing. Information resource sharing system is a highly complex information system, which requires better flexibility. Dynamic, distributed and intelligent systems are the best choice to support information resource sharing. However, such a system has high uncertainty, so it is necessary to give the reliability evaluation of information resource sharing system. The reliability of the product refers to the ability of the product to complete the specified functions under the specified conditions and within the specified time (or operation times). The reliability of products is similar to that of information resource sharing system. The following definitions are given for reliability of information resource sharing system:

Definition 1: the reliability of information resource sharing system refers to the ability of information resource sharing system to complete specified tasks under specified conditions and within specified time.

Definition 2: the reliability of information resource sharing system refers to the probability that the information resource sharing system can complete the specified functions under the specified conditions and within the specified time.

4 Establishment of Education Resource Database Based on Blockchain

According to the different transmission speed and form of educational resources, educational resources sharing can be divided into two modes: centralized mode and non centralized mode; Resource management without central mode takes decentralized supervision as its operation mode, and mainly uses point-to-point technology to realize sharing mode, which has the characteristics of convenient management and high data security [2–6]. On the basis of fully considering the respective advantages of the two modes, this paper constructs a network structure of digital education resource database with centralized supervision and no central structure, as shown in Fig. 1.

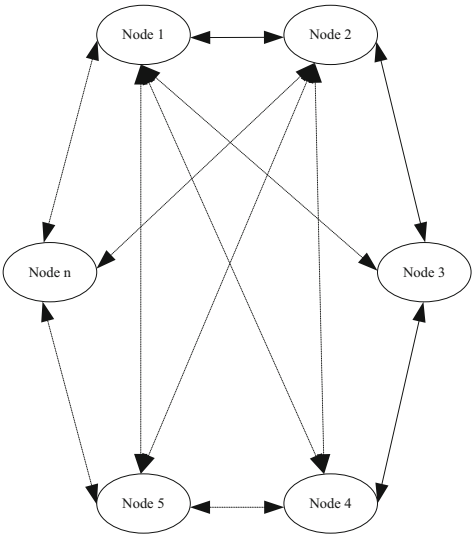

Fig. 1. Teaching resource database structure based on blockchain Technology

Among them, the nodes of the blockchain are sequential, and the node serial number is one of the basic attribute information of the block. In the framework of digital education resource sharing network structure, the main body of each node can be school teachers, training institutions or learners, and the nodes can be connected with each other. At the same time, in the framework model of digital education resources, blockchain technology is used as the underlying framework, and consensus mechanisms such as encryption algorithm, rule verification, digital signature and education smart contract system with high technical maturity are used to realize specific operations such as automatic loading, downloading and updating of education resources. Therefore, based on the principle of blockchain, this paper constructs a dynamic extensible, manageable, controllable and open service blockchain digital education resource database model, as shown in Fig. 2.

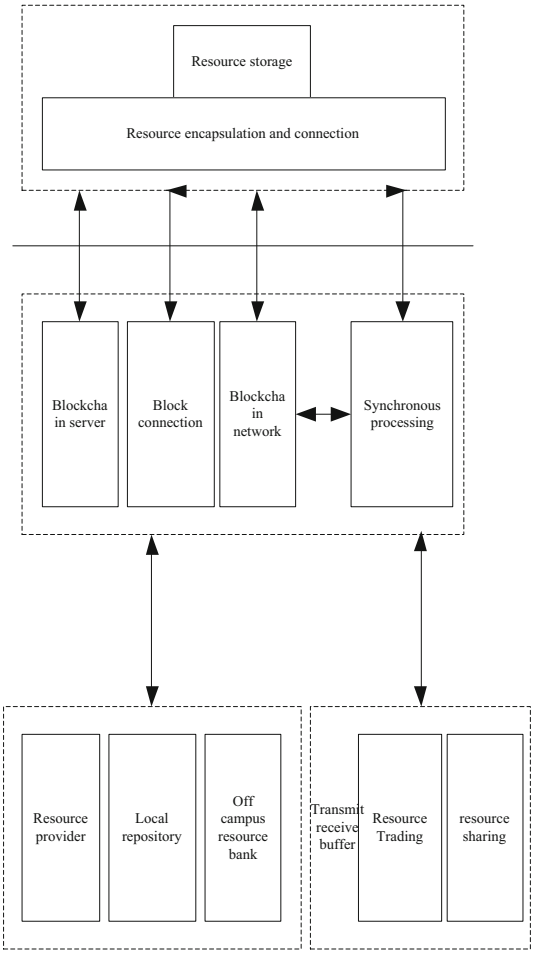

Fig. 2. Database structure

The blockchain digital education database model mainly includes four layers. ① Resource storage layer. First of all, we need to form books, videos, files and other educational resources into digital resources and encapsulate them in the form of blocks, and send them to local resources (servers). ② Resource connection layer. The packaged block resources form a block interconnection group through consensus mechanism and encryption algorithm, and are synchronized and updated in the network resource library. ③ Resource transaction layer. The resource provider encapsulates the digital resource in the block waiting for verification [7–15] (the basic data required in the block is shown in Table 1).

Table 1. Basic data in block

Serial number	Block data type	Explain
1	Node number	Node serial number is also the basic attribute information of block
2	Version number	Identification number of block version
3	Block size	Bytes representing data
4	Time stamp	A sequence of characters that uniquely identifies the time of a moment
5	Block address value	It is stored in block head, and is mainly obtained by hash algorithm SHA-256
6	Merkel root	A hash binary tree, invented by Ralph Merkle in 1979
7	Other information	Block related information, including information of resource provider, etc.

Then, the system connects each block to the main chain of the previous block in the blockchain system, and backs up the data information in each blockchain to all nodes, that is, each node records all the data in the whole blockchain. The block contains basic data information such as version number, time stamp and block address value, which makes clear the ownership of digital education resources. In case of infringement, each node can act as a "witness". ④ Resource sharing layer. The local resource database and the off campus resource database adopt the tree topology structure to save the data information of each node, so as to further improve the query speed of data information. As can be seen from Fig. 1 and Fig. 2, the digital education resource database established in this paper is a B2B network spontaneously formed by each node according to the demand for education resources. Learners, school teachers and training institutions can become a specific node in the blockchain network system after a series of security verification such as encryption algorithm, rule verification and digital signature. Network node is the core foundation of system operation, which is mainly responsible for generating blocks and forming blockchain network through hash algorithm connection. The specific connection process is shown in Fig. 3.

It can be found that the block head and block body constitute the basic structure of the block. Among them, the block head mainly includes the root value of Merkel tree, time stamp, difficulty value and other specific basic data information, and the block body usually contains multiple transaction records.

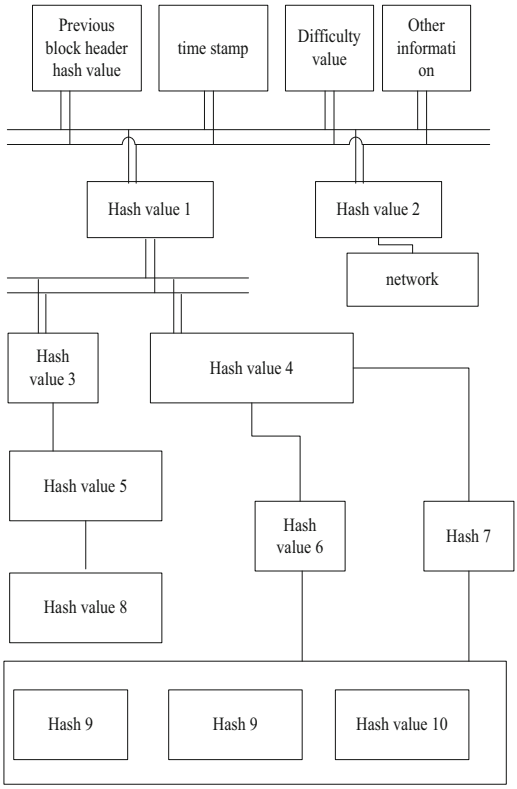

Fig. 3. Block structure of connection system

5 Reliability Evaluation Model of Educational Resource Sharing

5.1 Information Denoising

If there is noise in the reliability signal of network resource sharing system, it will have a certain impact on the evaluation results. It is necessary to denoise the reliability signal of the system. The following is the specific research process: the continuous form of wavelet function is given by using formula (1):

$$\Phi_{a,b}(t) = |a|^{-M/2}\Phi\left(\frac{t-b}{a}\right) \tag{1}$$

In the formula, a is the correlation coefficient of wavelet coefficients, b is discretized, Φ is scale parameter, M is denoising parameter.

5.2 Determination of Risk Assessment Method

Risk analysis is a method that teaching resource sharing system can systematically assess the risk of information security in the process of operation, and determine the level of risk based on it. It mainly includes qualitative analysis and quantitative analysis (including semi quantitative analysis) as shown in Table 2. Considering the complexity and cost [16–20], both qualitative analysis and quantitative analysis are very high, and quantitative analysis is more than qualitative analysis.

Table 2. Risk assessment method

Serial number	Method	Primary coverage
1	Qualitative analysis	Use text or descriptive data ranges to describe the magnitude of potential risks and the likelihood of occurrence of these risks
2	Semi quantitative analysis	In semi-quantitative analysis, the numerical range of qualitative analysis is known value, and the number referred to in each description may not be able to accurately represent the actual degree of risk influence semi-quantitative analysis or possibility. The purpose of semi-quantitative analysis is to obtain a more detailed degree of risk than qualitative analysis, but does not need to propose any actual value of risk obtained in quantitative analysis
3	Quantitative analysis	Quantitative analysis uses numerical value in the analysis of influence or possibility, while non quantitative analysis is the narrative numerical range applicable to qualitative or semi quantitative analysis, and uses data obtained from various sources and channels. The quality of quantitative analysis depends on the accuracy and integrity of the data used

At present, the risk assessment of teaching resource sharing system is mostly entrusted to security product manufacturers. It is difficult to determine the security requirements such as what to protect, where to protect the boundary of the object, and how much to protect. The establishment of evaluation methods must take into account the conditions and regulations of the teaching resource sharing system, such as the established scope of information security management system, information security implementation requirements, laws and regulations to be followed in the operation process, so as to achieve the effect and improve the efficiency. Based on the risk assessment of their own safety, a suitable quantitative analysis method in the process of being selected is mainly based on the evaluation of the effect, workload, cost and benefit, technical complexity and the difficulty of data collection.

Identification and Evaluation of Reliability

Within the scope of information security management system, teaching resource sharing system should be able to identify the assets, the principals, the elements of threatening assets, which weaknesses may be threatened to be used, and the potential impact on assets when availability, confidentiality or integrity are lost. Assess the security failures that may lead to commercial impact based on the potential impact of identified assets; Based on the main threats, weaknesses and impacts of assets, and the control measures being implemented, the realistic possibility of failure caused by such causes is evaluated; According to the established risk level criteria, the risk level is determined.

The Relationship Between the Elements of Reliability Evaluation

The work of reliability assessment must focus on the basic elements of assets, threats to information security, vulnerability in the process of information security implementation, security measures and risks. In the evaluation process of these elements, we must give full consideration to the related attributes, including the implementation of business development strategy, asset value, the events that affect the security in the development process, and the residual risks after. The relationship between the relevant elements in the risk assessment is shown in the figure, and the terms are explained in the table. In the figure, the basic element content is represented in the box, and the attribute content is represented in the ellipse. The relationship among the elements of reliability evaluation is shown in Fig. 4 below.

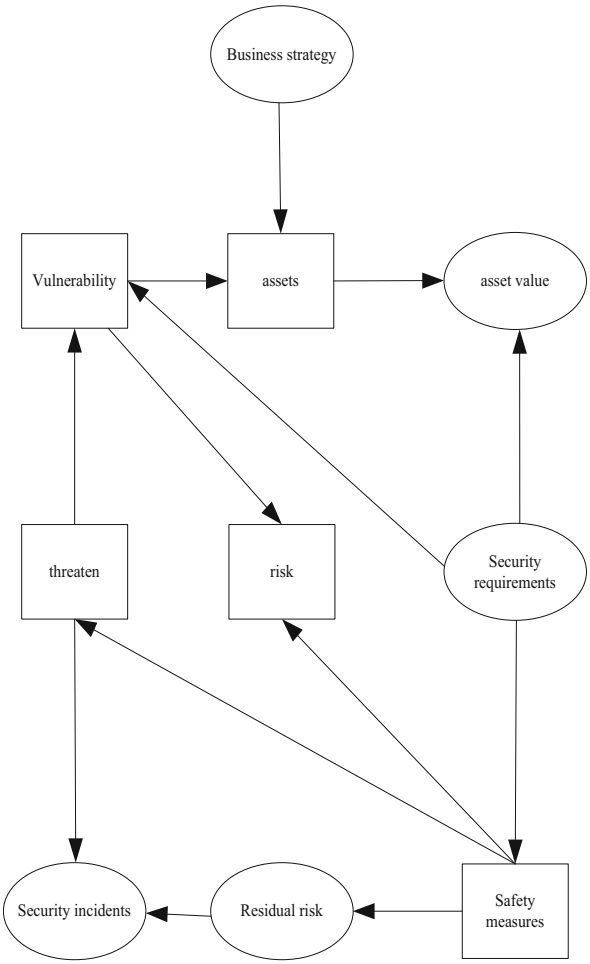

Fig. 4. Relationship of various elements of risk assessment

Table 3 below is a glossary of terms:

Table 3. Glossary

Serial number	Name	Primary coverage
1	Business strategy	The tasks of an organization realized by means of information technology
2	Assets	Anything of value to the unit
3	Asset value	Importance and sensitivity of assets
4	Threaten	Potential causes of accidents that may cause damage to assets or units
5	Risk	Due to the vulnerability of the system, the possibility and impact of security incidents caused by man-made or natural threats
6	Residual risk	After the safety protection measures are taken and the protection ability is improved, the possible risks still exist
7	Security incidents	If the threat subject can produce a threat and make use of the vulnerability of assets and their security measures, then the actual harm situation is called a security event

Reliability Evaluation Model Construction

Each element in the reliability evaluation model has its own unique attributes. In the process of calculating the reliability value, the first thing is to know the value of assets; The vulnerability of information assets is identified and its severity is assigned; Analyze the threat and its frequency; Fourth, the probability of security incidents is calculated according to the frequency and vulnerability of threats; Finally, the reliability is calculated according to the importance of information assets and the probability of security events on the information assets. The qualitative analysis of vulnerability is basically that the suppliers of products provide non teaching resource sharing system, which will hinder the determination of security requirements. The frame is shown in Fig. 5 below.

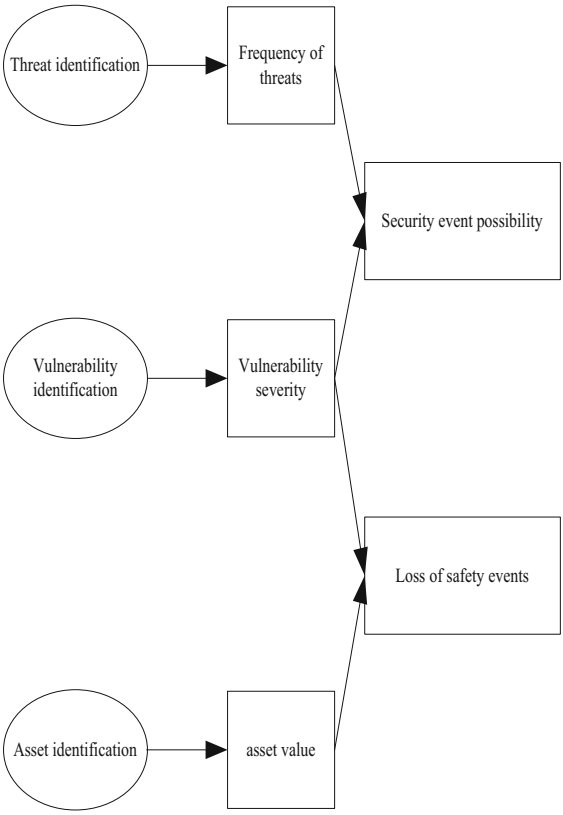

Fig. 5. Schematic diagram of risk assessment model

Reliability is one of the key factors in the design, research and operation of information resource sharing system. Due to the limitation of resources, such as cost, reliability and time, the optimization of system reliability has attracted extensive attention. For this reason, taking three optimization objectives of reliability, cost and time as examples, the multi-objective mathematical programming of workflow system reliability optimization is established, as shown in the following formula:

$$\left.\begin{array}{c} \max R(R_1, R_2, \cdots, R_N) \\ \min C(R_1, R_2, \cdots, R_N, T_1, T_2, \cdots, T_N) \\ \min T(T_1, T_2, \cdots, T_N) \\ s.t. R(R_1, R_2, \cdots, R_N) > R_{\min} \\ C(R_1, R_2, \cdots, R_N) > C_{\max} \\ T(T_1, T_2, \cdots, T_N) > T_{\max} \\ R_{i,\min} < R_i \cdot R_{i,\max} \end{array}\right\} \tag{2}$$

In formula (2), the reliability of system R and the cost of system C are also functions of the reliability and time of each unit; $R_{\min}$ is the lower bound of system reliability; $C_{\max}$ is the upper bound of system reliability; $T_{\max}$ is the upper bound of system time; $R_{i,\max}$. The upper and lower limits of the reliability of $R_{i,\min}$ element are constrained.

At the same time, in the actual network environment, the failure probability of the platform link and node is random and independent, and has known failure probability. The evaluation method of service platform reliability is mainly used to study whether the platform signal is stable and reliable. In the practical application network, for the irreparable information consulting service platform, the platform signal experiences the process of reliability decline until the communication of each signal fails. For repairable system, it will automatically enter the repair state after failure.

With the improvement of the reliability of hardware components in service platform. The average time of failure free is also increasing, CPU, memory and so on have a certain life cycle. When these hardware components are integrated to form communication links and nodes of the platform, the MTBF of the reliability signal of the consulting service platform is expressed as:

$$R_s = \left(\sum_{N}^{k=l} \frac{1}{R_k} \right)^{-1} \tag{3}$$

In formula (3), R_k represents the MTBF of component K in the service platform, and N represents the number of components in the service platform. Intuitively, the most unreliable component in the service platform determines the quality of the reliability signal of the whole service platform. Although the reliability of the whole platform is constantly improving, the integration of the platform is also increasing. A large number of platform components will lead to the decline of platform signal reliability.

Before the service platform is officially used, it is necessary to select qualified service platform components after the probation period and aging period. According to the energy description chart of service platform failure rate, the Weibull function is used to represent the failure rate curve $\alpha(t)$:

$$\alpha(t) = \begin{cases} 0, 0 \le t \le t_0 \\ \frac{a}{b}(t + c - t_l)^{\alpha}, t_0 \le t \le t_2 \\ \alpha, t_1 \le t \le t_2 \\ \frac{a}{b}(t - t_2)^{\alpha} + \alpha, t_2 \le t \end{cases} \tag{4}$$

In formula (4), a, b and c represent different shape coefficients. By measuring the failure rate of platform reliability signal at any time by actual failure measurement rate, the following failure rate is obtained at time t_1:

$$\alpha = \frac{a}{b} c^{\alpha} \tag{5}$$

In the actual network, the node and link efficiency of information consulting service platform mainly refers to the ratio of the current ability of node and link to complete the platform task to its maximum efficiency. In a non repairable system, the performance is expressed as follows:

$$E(t) = \exp\left(-\int_0^l \alpha(t)dt\right) \tag{6}$$

The network model is used to analyze the current network efficiency, and the premise of calculating network efficiency is to ensure the effectiveness of the network. Network efficiency is obtained by using all nodes and link efficiency in the network through topology performance, then network performance $E_N(t)$ is expressed as:

$$E_N(t) = E_e(t)E_v(t) \tag{7}$$

In formula (7), $E_v(t)$ represents the total node efficiency of the network resource sharing information consulting service platform, and the network efficiency is to ensure that each node in the network is effective. If the performance of a node in the network is 0, then $E_v(t)$ can be expressed as:

$$E_v(t) = \prod_n^{i=l} E_{vi}(t) \tag{8}$$

In the above formula (8), $E_{vi}(t)$ represents the efficiency of node c, and n represents the number of nodes of the network resource sharing information consulting service platform.

The Solution of the Model

The target lower limit $R_{\min}$ for the reliability of information resource sharing system is given. The target upper limit $R_{\max}$ of system reliability can be obtained by the following optimization model of maximum reliability which satisfies the cost constraints:

$$\left.\begin{aligned} &\max R(R_1, R_2, \cdots, R_N) \\ &s.t.C(R_1, R_2, \cdots, R_N) > C_{\max} \\ &T(T_1, T_2, \cdots, T_N) > T_{\max} \\ &R_{i,\min} < R_i \cdot R_{i,\max} \\ &T_i > 0 (i = 1, 2, \cdots, N) \end{aligned}\right\} \tag{9}$$

The target upper limit of information resource sharing system cost has been given. The target lower limit of system cost can be obtained by the following formula:

$$\left.\begin{array}{l}\min C(R_1, R_2, \cdots, R_N, T_1, T_2, \cdots, T_N) \\ s.t.R(R_1, R_2, \cdots, R_N) > R_{\min} \\ T(T_1, T_2, \cdots, T_N) < T_{\max} \\ R_{i,\min} < R_i \cdot R_{i,\max}\end{array}\right\} \tag{10}$$

The objective satisfaction function takes the objective function as the independent variable, and the target satisfaction represents the satisfaction degree of the decision-maker with the value of the objective function. The value of 1 indicates the most satisfied and the value of 0 indicates the most dissatisfaction. The specific process is shown in Fig. 6 below:

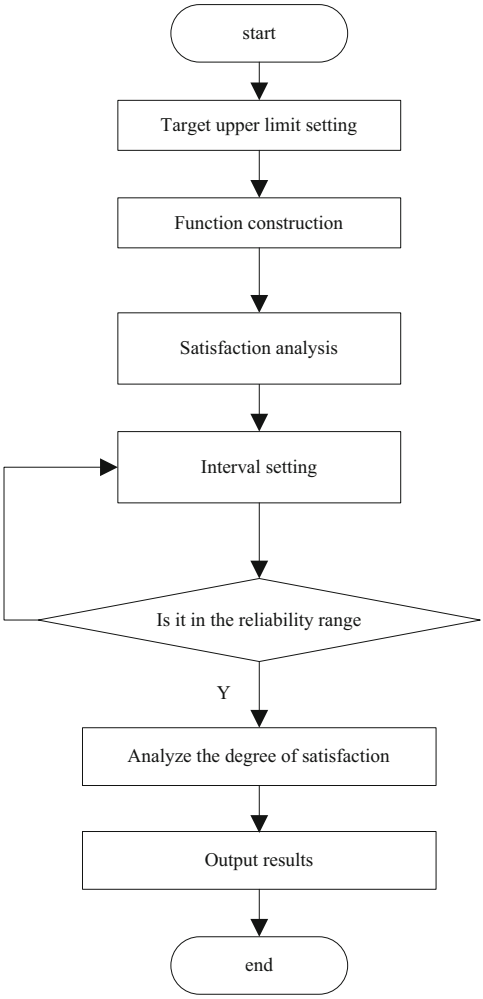

Fig. 6. Satisfaction calculation process

In general, it can be considered that in the system reliability tolerance interval $[R_{\min}, R_{\max}]$, the information resource sharing system reliability is the most satisfactory with the upper limit value $R_{\max}$, that is, the satisfaction degree of $R_{\max}$ is 1; And the reliability of information resource sharing system is the lowest limit, $R_{\min}$ is the most dissatisfied, that is, the satisfaction of $R_{\min}$ is 0.

The satisfaction function $h_1(R)$ of the reliability of information resource sharing system is a monotonic increasing function with the value in the interval $[0, 1]$. generally, it should be in the form of the following Fig. 7:

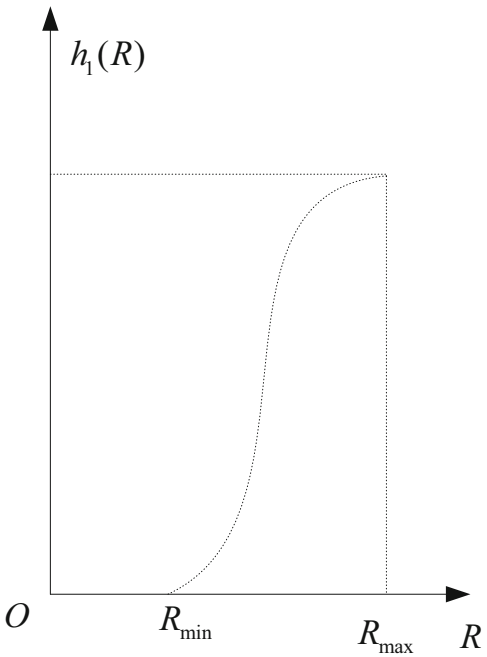

Fig. 7. Reliability satisfaction function

Through the above process, the reliability of online education resources sharing is detected.

6 Experimental Comparison

In order to verify the comprehensive effectiveness of the reliability detection method of online education resource sharing based on blockchain, simulation experiments are needed. Experimental environment: Visual Studio 2008 platform under win7 system, Intel Xeon processor, 4 GB memory, NVIDIA Quadro fx1800 display card. And the traditional detection method and the research method are compared to compare the detection effect of the two methods.

6.1 Comparison of Detection Efficiency

The comparison results of detection efficiency of the two methods are shown in Fig. 8.

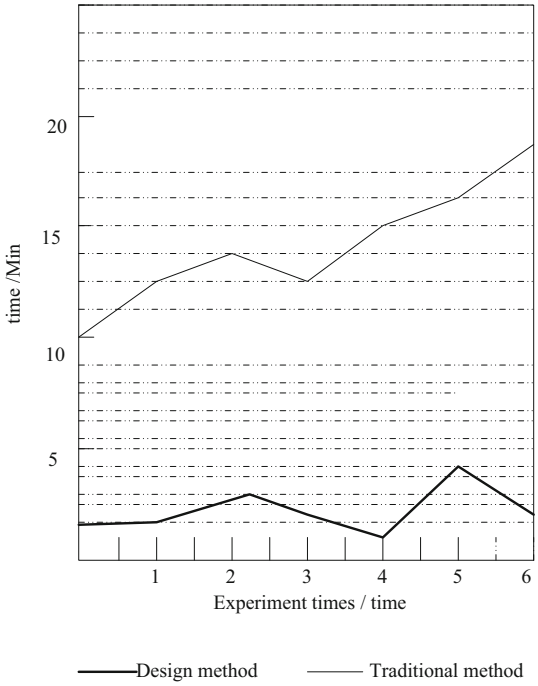

Fig. 8. Comparison of detection efficiency

Through the analysis of the figure above, it can be seen that the detection time of the reliability detection method in this study is less than that of the traditional method, which proves that the method in this study has higher detection efficiency.

6.2 Security Comparison of Educational Resources Sharing

The comparison results of the security of educational resource sharing between the traditional method and the studied method are shown in Fig. 9 below.

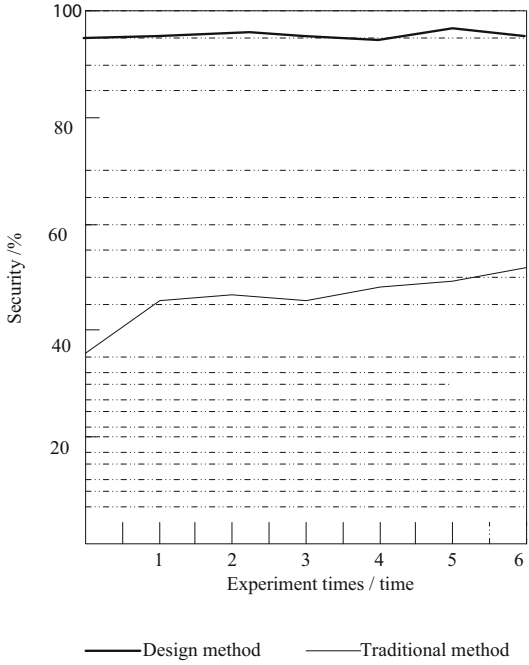

Fig. 9. Security comparison of educational resources sharing

Through the analysis of the above content, it is found that the sharing security result of this research method is higher than that of traditional methods, which has a certain practical significance.

7 Concluding Remarks

To sum up, the reliability detection method in this study can overcome the vulnerability of information resource sharing system, quantitatively analyze the reliability of information resource sharing system, improve the reliability of system, and prevent unreliable factors. It can provide a scientific basis for improving the security and reliability of the system, and the related theories, sharing models and applicable software development of information resource sharing system still need to be further studied.

References

1. Tan, G., Straub, N., Kaczmarek, S., Henke, M.: Blockchain-technologie im interdisziplinren umfeld. ZWF Zeitschrift fuer Wirtschaftlichen Fabrikbetrieb **114**(10), 605–609 (2019)
2. Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Qayyum, Z.U.: Docschain: blockchain-based IoT solution for verification of degree documents. IEEE Trans. Comput. Soc. Syst. **7** (3), 827–837 (2020)

3. Hameed, S., Shah, S.A., Saeed, Q.S., Siddiqui, S., Draheim, D.: A scalable key and trust management solution for iot sensors using SDN and blockchain technology. IEEE Sens. J. **21**(6), 8716–8733 (2021)
4. Kim, H.M., Laskowski, M., Zargham, M., Turesson, H., Kabanov, D.: Token economics in real life: cryptocurrency and incentives design for insolar's blockchain network. Computer **54**(1), 70–80 (2021)
5. Navy, S.L., Nixon, R.S., Luft, J.A., Jurkiewicz, M.A.: Accessed or latent resources? Exploring new secondary science teachers' networks of resources. J. Res. Sci. Teach. **57**(2), 184–208 (2020)
6. Han, J., Kim, D.: Security offloading network system for expanded security coverage in ipv6-based resource constrained data service networks. Wirel. Netw. **26**(6), 4615–4635 (2020)
7. Fan, P., Liu, Y., Zhu, J., Fan, X., Wen, L.: Identity management security authentication based on blockchain technologies. Int. J. Netw. Secur. **21**(6), 912–917 (2019)
8. An, Y., Xu, M., Shen, C.: Classification method of teaching resources based on improved knn algorithm. Int. J. Emerg. Technol. Learn. (iJET) **14**(4), 73–88 (2019)
9. Yi, B., Wang, X., Huang, M., Yang, L.: Cost and security-aware resource allocation in optical data center networks. IEEE Commun. Lett. **23**(11), 2031–2035 (2019)
10. Yang, W., Zhao, X., He, J.: Physical layer security and energy efficiency driven resource optimisation for cognitive relay networks. IET Commun. **14**(17), 2953–2961 (2020)
11. Kibiwott, K.P., Zhang, F., Kimeli, V.K., Anyembe, O.A., Opoku-Mensah, E.: Privacy preservation for ehealth big data in cloud accessed using resource-constrained devices: survey. Int. J. Netw. Secur. **21**(2), 312–325 (2019)
12. Bai, X., Li, J.: Intelligent platform for real-time page view statistics using educational big data digital resource sharing. J. Intell. Fuzzy Syst. **40**(1), 1–10 (2020)
13. Yuan, Q.: Network education recommendation and teaching resource sharing based on improved neural network. J. Intell. Fuzzy Syst. **39**(4), 5511–5520 (2020)
14. Wittmann, M.C., Millay, L.A., Alvarado, C., Lucy, L., Rogers, A.: Applying the resources framework of teaching and learning to issues in middle school physics instruction on energy. Am. J. Phys. **87**(7), 535–542 (2019)
15. Liu, S., Bai, W., Zeng, N., Wang, S.: A fast fractal based compression for MRI images. IEEE Access **7**, 62412–62420 (2019)
16. Pender, L.K., Kadkhoda, H., Lucero, K.S., Repetto, P., Weber, J.S.: Effects of online education on the identification and management of immune-related adverse events over time. J. Clin. Oncol. **37**(15), 18224 (2019)
17. Liu, S., Pan, Z., Cheng, X.: A novel fast fractal image compression method based on distance clustering in high dimensional sphere surface. Fractals **25**(4), 1740004 (2017)
18. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., Zhang, Y.: Blockchain and deep reinforcement learning empowered intelligent 5g beyond. IEEE Netw. **33**(3), 10–17 (2019)
19. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mob. Netw. Appl. **24**(1), 5–17 (2018). https://doi.org/10.1007/s11036-018-1134-8
20. Luo, B., Li, X., Weng, J., Guo, J., Ma, J.: Blockchain enabled trust-based location privacy protection scheme in vanet. IEEE Trans. Veh. Technol. **69**(2), 2034–2048 (2020)