Hindawi
Journal of Electrical and Computer Engineering
Volume 2022, Article ID 9781939, 1 page
https://doi.org/10.1155/2022/9781939

Retraction

Retracted: The Security of Student Information Management System Based upon Blockchain

Journal of Electrical and Computer Engineering

Received 22 November 2022; Accepted 22 November 2022; Published 20 December 2022

Journal of Electrical and Computer Engineering has retracted the article titled "The Security of Student Information Management System Based upon Blockchain" [1] due to concerns that the peer review process has been compromised.

Following an investigation conducted by the Hindawi Research Integrity team [2], significant concerns were identified with the peer reviewers assigned to this article; the investigation has concluded that the peer review process was compromised. We therefore can no longer trust the peer review process, and the article is being retracted with the agreement of the Editorial Board.

The author does not agree to the retraction.

References

[1] M. Yang and J. Wang, "The Security of Student Information Management System Based upon Blockchain," *Journal of Electrical and Computer Engineering*, vol. 2022, Article ID 8186189, 9 pages, 2022.

[2] L. Ferguson, "Advancing Research Integrity Collaboratively and with Vigour," 2022, https://www.hindawi.com/post/advancing-research-integrity-collaboratively-and-vigour/.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2022, Article ID 8186189, 9 pages
https://doi.org/10.1155/2022/8186189

Research Article

The Security of Student Information Management System Based upon Blockchain

Mingfeng Yang[1] **and Jianying Wang**[2]

[1]*Business Administration School, Zhejiang Technical Institute of Economics, Hangzhou 310018, Zhejiang, China*
[2]*Laboratory and Equipment Management Department, Zhejiang University of Water Resources and Electric Power, Hangzhou 310018, Zhejiang, China*

Correspondence should be addressed to Mingfeng Yang; ymf@zjtie.edu.cn

Received 4 March 2022; Revised 31 March 2022; Accepted 9 April 2022; Published 21 April 2022

Academic Editor: Wei Liu

In recent years, with the development of science and technology, as an emerging data security technology, blockchain has been widely used in all walks of life by virtue of its immutability, uniqueness, smart contract, and decentralized organization. Examples include industry, services, and education. With the progress of China's education, the application of blockchain technology in the field of education has also been further expanded. At present, the application of blockchain in China's education field is mainly concentrated in three areas: education resource management, teaching information management, and education basic platform construction. This article aims to study the security of the student information management system based on the blockchain. The security test experiment of the student information management system is carried out based on the encryption algorithm of the blockchain, and conclusions are drawn. The security of the student information management system based on the encryption algorithm of blockchain technology has increased by 87%, which also shows that the blockchain technology has a better effect on improving the security of the student information management system.

1. Introduction

In today's era, with the improvement of social science and technology and the development of education, education and teaching are becoming more and more intelligent and informatized. Educational informatization refers to the application of modern information technology to teaching management and scientific research and pays attention to the development and utilization of educational information resources. Educational intelligence and informatization have greatly improved the efficiency of the teaching process and the ability to manage and share educational resources, thereby continuously promoting the continuous development of education. However, in the process of informatization teaching and educational resource management, a large amount of information about education, teaching, and personal privacy of students will be involved. If the information is stored and managed improperly, it will lead to the leakage of important information in the education and teaching process and the leakage of students' personal privacy. This will have a huge negative impact on the education and teaching process and the protection of student privacy, and it will also pose a certain threat to the entire education and social security. Therefore, in a modern society where privacy protection issues are increasingly prominent, there is an urgent need for a system technology that combines security, reliability, and privacy protection. It reasonably protects and manages important education and teaching information and student privacy information involved in the process of education and teaching informatization. The blockchain is a data structure that links some important related information and data blocks in chronological order. It was first applied in the Bitcoin field. Since the birth of Bitcoin in 2009, the Bitcoin blockchain has had thousands of distributed nodes around the world, and it has been running uninterruptedly for nearly 10 years without

major security breaches. Although blockchain technology originated from encrypted digital currency, its development and application are not limited to the financial field. It can be widely used in many aspects and fields such as culture and entertainment, social welfare, and data protection. Because the blockchain combines technologies and algorithms such as economic design, cryptographic encryption algorithms, and distributed network technology, it can ensure the integrity, reliability, uncodable modification, and uniqueness of information and data on the blockchain, thereby ensuring maximum protection of private data security. These characteristics and advantages of blockchain technology make it also have a certain application value in the education field, and it is more widely used in the education industry and other industries.

The application value of blockchain technology in various fields has caused a lot of research on blockchain technology to emerge in academia. For example, Miraz and Ali's research puts forward that blockchain technology is the key supporting technology behind the Bitcoin cryptocurrency system, and blockchain technology also plays a vital role in other application fields that need to ensure the security of private data. Therefore, their research mainly tested and evaluated the actual application effects of the blockchain plan in various fields and found that the blockchain technology has good application effects in various fields [1]. Yeoh studied the technical regulatory challenges of blockchain technology in the EU and the United States. That research is based on the main data of applicable regulations and auxiliary data in the public domain, including relevant case study explanations. It came to the conclusion that the smart regulatory noninterference approach adopted by blockchain technology in the EU and the United States indicates that blockchain technology will become more inclusive in financial services and related fields in the future [2]. Benchoufi and Ravaud's research focuses on the application of blockchain technology in the field of clinical medicine. Their research concluded that blockchain technology is helpful to the challenges of personal data privacy and data sharing reproducibility of patient registration in clinical medical experiments [3]. Ittay mainly studied how blockchain technology can narrow the security and privacy gap in the neighborhood outside the Bitcoin field and proposed that blockchain technology has high potential application value for the financial industry [4]. Saberi et al. studied the application of blockchain technology in government public decision-making and concluded that blockchain technology can directly affect government investment decisions through some very important information [5]. Efanov and Roschin proposed that, in today's society, blockchain technology is considered to be the most important invention after the Internet. They mainly studied the peer-to-peer network technology of blockchain technology and the application of public key cryptography and concluded that the application of these technologies in blockchain can solve any trust problem well [6].

Although the fields are all related to blockchain technology and its practical applications, corresponding research conclusions have also been drawn. However, the research perspectives and content of these studies are not broad enough, and they all have certain limitations. The innovation of this article lies in the following: Combined with block chain technology and its encryption algorithm, this paper carries out a detailed and effective security test experiment on student information management system based on block chain technology and gets students' research on encryption algorithms based on blockchain technology. The results show that the security of the information management system is improved by 87%. It provides application value reference for the application of blockchain technology in student information management system.

2. Research Methods on the Security of Student Information Management Systems

2.1. Blockchain Technology

2.1.1. Basic Concepts of Blockchain Technology. Blockchain is an emerging data security technology. It can also be said to be a distributed ledger that shares data between points in a peer-to-peer network [7]. Blockchain itself is not a brand-new technology but a combination of a variety of existing technologies, involving cryptography, probability theory, consensus mechanism, and distributed network as well as other computer technologies. The nodes in the distributed network of the blockchain jointly maintain public data in a trustless and decentralized manner. There can be any number of nodes in the blockchain, and each node needs to follow the same consensus mechanism to continuously generate new blocks at a certain time interval. Each new block joined together creates a new chain of information. During this time, the data records in the blockchain will be stored there. There are many kinds of blockchain consensus mechanisms, and the working methods of blockchains of different consensus mechanisms are quite different. The blockchain consists of a series of blocks connected in sequence. These blocks contain a timestamp and are connected by the hash value of the previous block. The cleverly designed block structure based on cryptography ensures that the block is sealed in a safe and unsealed way [8, 9]. The blockchain structure is shown in Figure 1.

2.1.2. Blockchain Classification. Blockchains can be divided into public chains, private chains, and consortium chains according to their nature and usage [10, 11]. The data in the public chain are open to the public. Anyone in the public chain can participate in the data consensus process and can act as a simple node or absentee node. The private chain is controlled by an organization, and the centralized manager determines the role and management authority of the node. The private chain information is not public, and only a small number of internal relevant personnel can see and use it. The consortium chain is between the public chain and the private chain. Some preselected nodes participate in the data consensus process of the consortium chain. The members of the

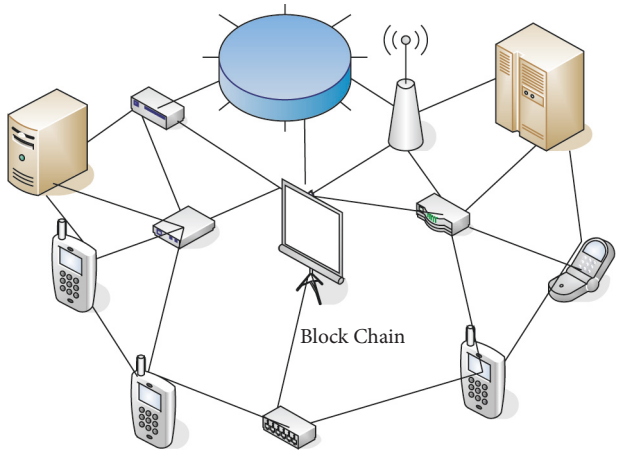

Figure 1: Blockchain structure.

consortium chain have specific access rights and are jointly maintained by several organizations [12, 13]. Blockchain classification is shown in Table 1.

2.1.3. Blockchain Technology Workflow. Blockchain combines a variety of existing technologies [14, 15] to implement logic applications by creating and updating data, sending data between nodes, using automated script codes, or using smart contracts. If traditional databases can only maintain data security unilaterally, then blockchain can maintain data security in an all-round way. The blockchain workflow mainly includes three steps: block generation, consensus verification, and ledger maintenance, forming a complete blockchain operation process.

2.2. Blockchain Encryption Algorithm. When the blockchain applicant has computing needs, the requester sends a computing request to the applicant. Then the applicant requests the kernel and auxiliary components to calculate the feedback value and secretly sends the feedback value to the requester [16, 17]. The applicant uses the verification key to determine the validity of the feedback value. After receiving n valid feedback values, the correct calculation result can be obtained.

The first step is initialization. F_a is a finite field characterized by a. The distributor randomly selects a polynomial $F(x)$ of degree n-1 with the following form in F_a (x):

$$F(X) = a_{n-1}x^{n-1} + a_1 x + S_{\text{core}}. \tag{1}$$

In the above equation, a_{n-1}, a_{n-2}, $s_{\text{core}} \in F_a$, and a is not zero; let

$$\begin{aligned} F(x) &= a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + a_1 x, \\ g(x) &= c_{n-1}x^{n-1} + c_1 x. \end{aligned} \tag{2}$$

Then calculate $h(x)$:

$$h(X) = (x)^2 - g(x) - b_{n-2}x^{n-2}. \tag{3}$$

That is,

$$h(x) = b_{2n-3}x^{2n-3} + b_1 x. \tag{4}$$

Then calculate and verify K:

$$K = g^{a_{n-1}} + g^{c_n}. \tag{5}$$

First, randomly select n different numbers $x_1, x_2, \ldots\ldots x_n \in F_p$. Then, from j to 1 to n, calculate

$$g_n^f = \left(g^{n-1}\right)\left(g^{n-2}\right). \tag{6}$$

That is,

$$g_n^f = g^{a_{x-1+a_{x-2}}} + g^{a_1 x}. \tag{7}$$

At the end of the second step, j is from 1 to n, if the following Formulas are all true:

$$e\left(g_j^f, g_j^f\right) = e\left(g_j^h, g_j^n\right). \tag{8}$$

Then K is valid; otherwise, reject this K and return to the first step.

$$CF_1 = F(ID)h(ID), \tag{9}$$

where $CF1$ is the information value before encryption. The distributor uses the public key K to encrypt CF_1 to obtain the encrypted value C_1^{eore}. The distributor sends it to Sr.

$$\text{Resp} = \left(CF_i + S_i\right)\left(CF_i + S_{i2}\right). \tag{10}$$

After that, Sr uses the public key K of the aggregator to encrypt ResP to obtain the ciphertext:

$$C_{\text{Resp}} = \text{Enc}_p\left(\text{Resp}_i\right). \tag{11}$$

Then Sr sends it to the aggregator.

Assume that the feedback value collected by the aggregator is Resp_i from 1 to n; the aggregator performs the following calculations:

$$CF_i = \left(g^{a_{i=1}}\right)\left(g^{a_{i=n}}\right). \tag{12}$$

The aggregator uses S and the bilinear mapping e to calculate the following formula:

$$\begin{aligned} E &= e\left(CF_i g s_n\right) e\left(CF_n\right), \\ F(X) &= \sum_{i=1}^{t} \text{Resp} \prod_{i=1}^{t} \frac{x - ID}{ID - ID_i}. \end{aligned} \tag{13}$$

In addition, it can also add the last step of inspection. Put the set encrypted number into the formula flow, compare the result with the one set by yourself, and verify the accuracy of the algorithm.

The entire blockchain encryption algorithm process is shown in Figure 2.

3. Security Test Experiment of Student Information Management System Based on Blockchain

3.1. Experimental Method. The main method of this experiment is as follows: First, select some academic data to

Table 1: Blockchain classification.

Attributes	Public chain	Alliance chain	Private chain
Participants	Anyone	Alliance member	Members in the organization
Read permission	Public	Public or restricted	Restricted
Consensus mechanism	Pow, PoS, dPoS	PBFS, RaFt	Solo PBFS
Efficient	Low	Low	High
Represent	Bitcoin	Hyperledger fabric	MultiChain

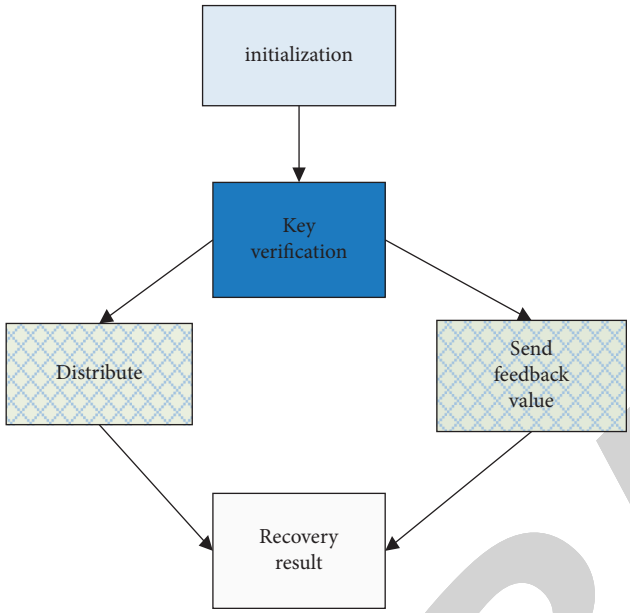

Figure 2: Blockchain encryption algorithm flow.

form an academic information model for the ordinary student information management system A that does not incorporate blockchain technology, and conduct a security test on it. Then, the student information management system of the same academic information model is combined with blockchain-based data protection technology and encryption algorithm to encrypt the information and then perform the system security test [18, 19]. Finally, the comparison is made and the experimental results are obtained.

3.2. Security Test of General Student Information Management System A. First, randomly select a part of the data from a large amount of academic data to build an academic information model. As the security test model of this ordinary student information management system, this article uses the security test model of the student information management system of blockchain technology and blockchain encryption algorithm. The selected academic data are shown in Table 2.

After the model is established, we will start to test the security of the ordinary student information management system A. The security test of the student information management system includes two aspects: one is the relationship between the length of the login password and the security of the account; the other is the evaluation of the difficulty of reading and transferring account information

Table 2: Academic data.

Field name	Type	Encryption method
Student ID	String	Symmetric encryption
Name	String	Symmetric encryption
Major	String	Symmetric encryption
Entity ID	String	Symmetric encryption
Phone	String	Symmetric encryption

[20]. Next, we first test the relationship between the length of the login password of the student information management system A and the account security. The test results are shown in Figure 3.

The next step is to determine the degree of difficulty of reading and transferring account information in system A. The result is shown in Figure 4.

From Figures 3 and 4, we can first see that the account security of system A is directly proportional to the length of the password. It shows that the account security of system A is closely related to the length of the login password. The longer the password, the stronger the account security. This situation is also in line with the actual system situation. Second, we can also see that as the number of readings of information increases, the amount of information read is also increasing. Moreover, with the increase in the number of times of information transfer, although the amount of transferred information has not increased much, it is also showing an increasing trend. These phenomena show that the difficulty of reading and transferring information in system A is not great, and the difficulty coefficient of transferring information is slightly higher. However, users can read and transfer more information easily by continuously reading and transferring. In summary, although the ordinary student information management system A has a certain degree of security, it is not very safe. Under this system, the security of the account is easily affected by the length of the password, and it is easier to read and transfer account information.

3.3. Security Test of Student Information Management System B Using Blockchain Technology. Next, we will conduct a security test of the student information management system B using blockchain data security technology. First of all, based on the same academic data model in Table 2, we combined it with blockchain technology and used the blockchain encryption algorithm to encrypt the important data in the system. Then update the system and retest the relationship between the account security of the new system B and the length of the login password, as well as the account information read and transfer difficulty coefficient

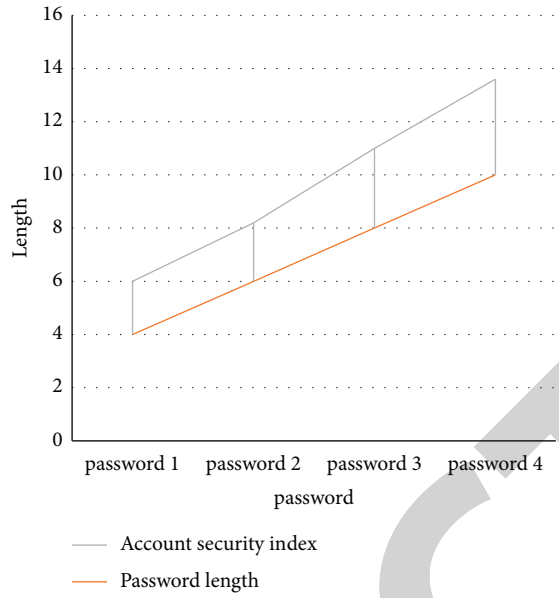

Figure 3: The relationship between the length of system A password and account security.

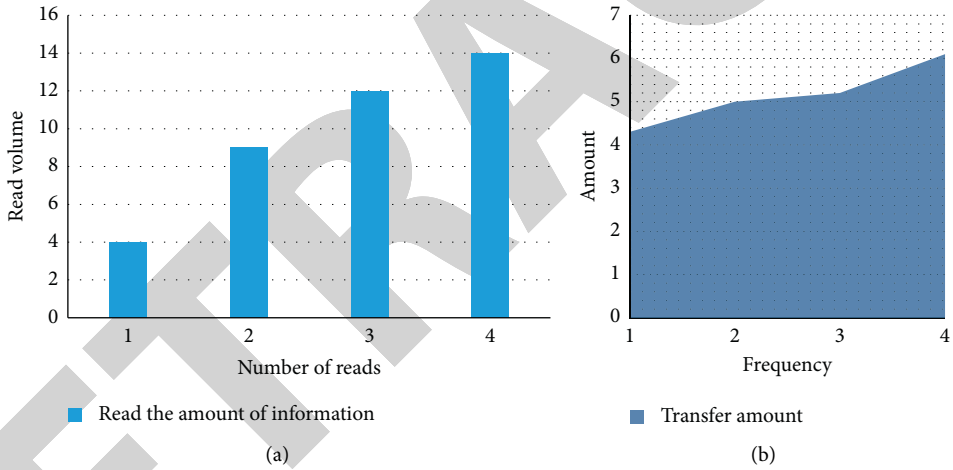

Figure 4: Difficulty of reading and transferring account information in system A. (a) Difficulty in reading information. (b) Difficulty in transferring information.

evaluation. The test results of the relationship between the account security and the password length of the student information management system B using blockchain technology are shown in Figure 5.

From Figure 5, we can see that the account security of the new student information management system B after the use of blockchain technology and blockchain encryption algorithms also has a certain proportional relationship with the length of the password. But, unlike system A, the account security and password length of system B do not maintain a proportional relationship from beginning to end. But when the password length reaches 6 characters, the account security will no longer increase as the password length changes. This shows that there is a fixed restricted value between account security and password length in the student information management system based on blockchain technology. That is, the account login password is required to be at least 6 digits. If this requirement is met, the security of the account is no longer affected by the length of the password but has always maintained stable security.

Next is the evaluation of the difficulty coefficient of reading and transferring account information of system B. The evaluation results are shown in Figure 6.

From Figure 6, we can see that the difficulty of reading and transferring account information in the new student information management system that uses blockchain data security technology is limited. That is, when the number of times of information reading and dumping reaches a certain value, the amount of information read and dumped is a fixed value and no longer changes. This shows that blockchain technology and blockchain encryption algorithms restrict the reading and transfer of account information in system B. When the number of reads and the number of transfers reaches a certain value, the system will automatically

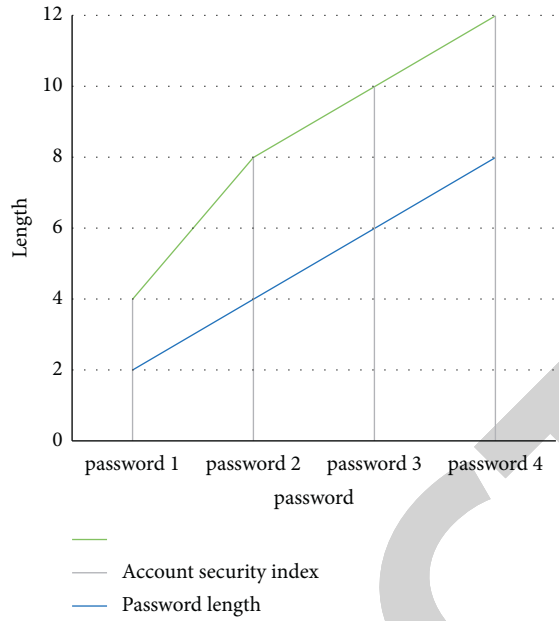

Figure 5: The relationship between account security and password length in system B.

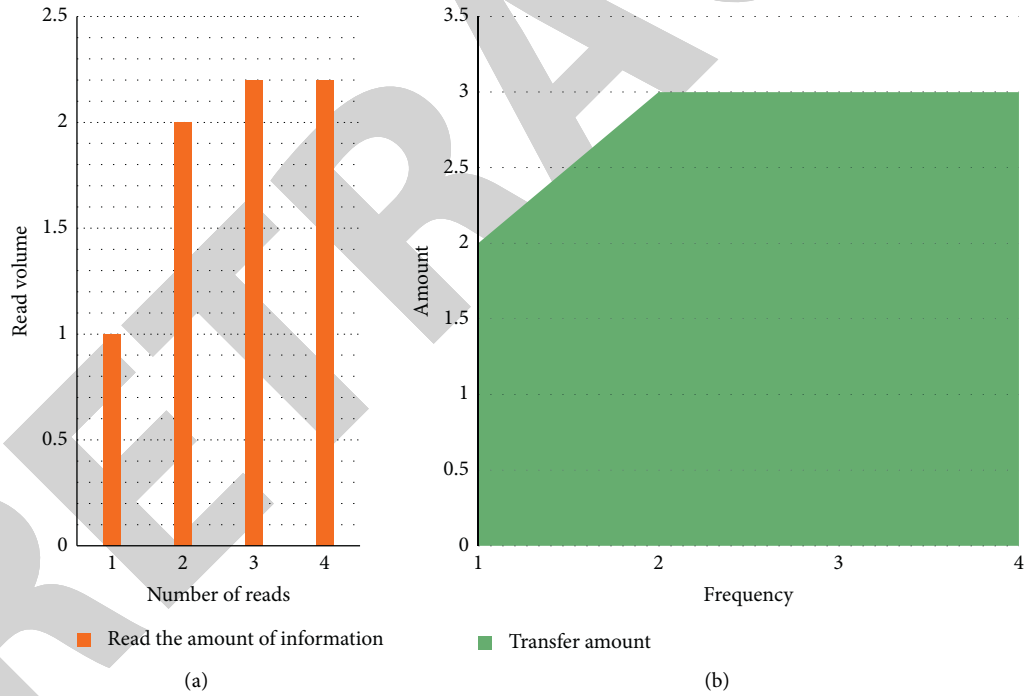

Figure 6: Difficulty of reading and transferring account information in system B. (a) Difficulty in reading system information. (b) Difficulty in transferring system information.

determine that the amount of account information read and transfer has reached the limit value. If it continues to extract and transfer, the system will determine that the account is at risk at this time and then encrypt and block the account information so that the user can no longer continue to extract and transfer the information of this account [21]. Therefore, when the blockchain technology and blockchain encryption algorithm are combined, the security of the new student information management system is greatly improved. After the evaluation data conversion calculation, the security of the student information management system B based on blockchain technology is 87% higher than that of the ordinary student information management system A that does not apply blockchain technology.

In summary, the conclusion of this experiment is that the security of the student information management system based on blockchain technology is 87% higher than that of the ordinary student information management system that

does not apply blockchain technology. This conclusion shows that blockchain technology and blockchain encryption algorithms have good application effects for the security and improvement of student information management systems.

3.4. Experimental Summary. At this point, the entire experimental process is complete. Finally, let us summarize this experiment. This experiment is based on the common student information management system A based on the same academic data model and the new student information management system B that combines blockchain data security technology. It tested the relationship between account security and password length and the difficulty of reading and transferring information to test the security of the two systems. The conclusion shows that the student information management system based on blockchain technology has high security. This experiment is relatively smooth on the whole and is proceeded step by step and finally reached effective conclusions. But we believe that this experiment still has room for improvement in terms of experimental methods and efficiency. It is hoped that future experiments can complete the experiment and draw conclusions with more standardized steps in a shorter time and at a faster speed.

4. Discussion

As an emerging data security technology, blockchain combines security, reliability, and privacy protection and can ensure the integrity, uniqueness, and codability of data. The blockchain technology also combines computer technology and segmented network technology. Advanced technologies and algorithms such as artificial intelligence technology and privacy encryption algorithms have powerful technical functions and technical advantages [22]. Therefore, blockchain technology has continued to develop and progress since its inception. Today, the scope of application in various fields is also expanding. The education neighborhood is an important field. In the process of informatization of education and teaching, such as the realization and application of student information management system, a reliable privacy protection technology is needed to protect a large amount of important education and teaching information and students' personal privacy information involved. Relying on its technical advantages, blockchain technology also has certain application value. This article assumes that the basic data storage protection and management technology of blockchain technology and the blockchain encryption algorithm have a certain effect on the security of the student information management system in the education field, and, based on this article, a security test experiment of student information management system based on blockchain is designed. In the experiment, blockchain technology and blockchain encryption algorithm are combined to evaluate the student information management system A that does not use blockchain technology and the student information management system B that uses blockchain technology. The content includes the relationship between account security and the length of the login password, as well as the difficulty of reading and transferring information. Based on this, this article has tested the overall security of the two systems. Finally, this article compares the security of the student information management system that uses blockchain technology with the security of the student information management system that does not use blockchain technology and finds that the security of the student information management system that uses blockchain technology has increased by 87%. Such experimental results show that blockchain technology has a certain role in improving the security of student information management systems.

5. Conclusions

In today's society, science and technology are advancing with each passing day, and all kinds of advanced science and technology have come out one after another. The emergence of advanced science and technology has promoted the technologicalization and advancement of the entire society and the world. The level of integration of science and technology in various industries and fields is also constantly improving, such as education informatization. Informatization of education is to modernize teaching methods, informatization of education dissemination, and teaching methods. In the process of education informatization, computer technology, multimedia technology, big data, artificial intelligence, and network information technology will be fully used. Among them, it will inevitably involve a large amount of important education and teaching information and personal private information of students, and this information or data need to be properly stored and managed. Therefore, one of the education and teaching information management systems that store and manage these data in an all-round way, the student information management system, appeared. The student information management system is a management system developed to reduce the school's large amount of business work in student information management. The student information management system is mainly used for school student information management. The main task and goal is to realize the systematization, scientification, and automation of student information storage and management. The student learning management system uses computers to properly store and manage various student information. With the continuous development of China's education and the continuous increase of the country's investment in the field of education, the student information management system has been implemented and applied in all aspects of society. Since the process of student information management system will involve a large amount of education and teaching information about students and personal privacy information, a reliable data security technology must be combined to ensure the security of student information management system. The blockchain technology is a data security technology that links some

important related information and data blocks in chronological order. It combines computer technology, economic design, cryptographic encryption algorithm, and distributed network technology and other technologies and algorithms and has strong data security management capabilities. Since its inception, blockchain technology has been used more and more widely in information security management in all walks of life. This article believes that blockchain technology also has a certain effect on the security of student information management systems. Based on this idea, this paper designs a security test experiment for student information management system based on blockchain. In the experiment, the security tests of the student information management system without blockchain technology and the student information management system combined with blockchain technology were conducted. Finally, this article compares the security of the student information management system with blockchain technology and the security of the student information management system without blockchain technology. It is found that the security of the student information management system that uses blockchain technology is 87% higher than that of the student information management system that does not use blockchain technology. Therefore, the experimental conclusion of this article is drawn: blockchain technology has a certain effect on improving the security of student information management system. This conclusion provides a certain reference value for the further application of blockchain technology in the security maintenance of student information management systems and also provides some reference for other research on the security of student information management systems based on blockchain technology. However, due to the limited research ability and level, the research of this article also has some limitations. Even so, academic research on blockchain technology and the security of student information management systems based on blockchain technology will not stop. In the future, there will surely be more outstanding research on the security of student information management systems based on blockchain technology, so as to continuously promote the development of blockchain technology and improve the security of student information management systems.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest with any financial organizations regarding the material reported in this manuscript.

References

[1] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1–6, 2018.

[2] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, 2017.

[3] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, pp. 335–35, 2017.

[4] E. Ittay, "Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[5] S. Saberi, M. Kouhizadeh, and J. Sarkis, "Blockchain technology: a panacea or pariah for resources conservation and recycling?" *Resources, Conservation and Recycling*, vol. 130, no. 30, pp. 80-81, 2018.

[6] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Computer Science*, vol. 123, no. 23, pp. 116–121, 2018.

[7] M. R. Biktimirov, A. V. Domashev, P. A. Cherkashin, and A. Y. Shcherbakov, "Blockchain technology: universal structure and requirements," *Automatic Documentation and Mathematical Linguistics*, vol. 51, no. 6, pp. 235–238, 2017.

[8] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 1, no. 32, pp. 815–823, 2018.

[9] R. Igor and L. Robert, "Opportunities for use of blockchain technology in medicine," *Applied Health Economics and Health Policy*, vol. 1, no. 6, pp. 1–8, 2018.

[10] K. J. Jang, "The A study on innovative financial services of business models using BlockChain technology," *The e-Business Studies*, vol. 18, no. 6, pp. 113–130, 2017.

[11] A. Tezel, E. Papadonikolaki, I. Yitmen, and P. Hilletofth, "Preparing construction supply chains for blockchain technology: an investigation of its potential and future directions," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 547–563, 2020.

[12] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Computing & Applications*, vol. 32, no. 3, pp. 639–647, 2020.

[13] Y. Li, J. Wei, J. Yuan, Q. Xu, and C. He, "A decentralized music copyright operation management system based on blockchain technology," *Procedia Computer Science*, vol. 187, pp. 458–463, 2021.

[14] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, "A survey of blockchain technology on security, privacy, and trust in crowdsourcing services," *World Wide Web*, vol. 23, no. 1, pp. 393–419, 2020.

[15] D. Zhang, "Application of blockchain technology in incentivizing efficient use of rural wastes: a case study on yitong system," *Energy Procedia*, vol. 1, no. 58, pp. 707–714, 2019.

[16] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain reengineering using blockchain technology: a case of smart contract based tracking process," *Technological Forecasting and Social Change*, vol. 144, no. 7, pp. 1–11, 2019.

[17] F. Casino, V. K Anakaris, T. K. Dasaklis, S. Moschuris, and N. P. Rachaniotis, "Modeling food supply chain traceability based on blockchain technology," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 728–733, 2019.

[18] L. Savron, "How blockchain technology could change our lives," *Ursidae: The Undergraduate Research Journal at the University of Northern Colorado*, vol. 8, no. 1, pp. 10–18, 2019.

[19] W. Zhao, "Blockchain technology:development and prospects," *National Science Review*, vol. 6, no. 02, pp. 193–197, 2019.

[20] S. Buonpane, "Blockchain technology's role in the risk management value chain," *Engineering news-record*, vol. 281, no. 12, p. 38, 2018.
[21] M. M. Zuberi, "A silver ('Chain') lining: can blockchain technology succeed in disrupting the banking industry?" *Banking and Financial Services Policy Report*, vol. 36, no. 3, pp. 1–4, 2017.
[22] P. Treleaven, R. Gendal Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.