Hindawi
Security and Communication Networks
Volume 2023, Article ID 9856127, 1 page
https://doi.org/10.1155/2023/9856127

Retraction

Retracted: Security Research in Personnel Electronic File Management Based on Blockchain Technology

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Wang and J. Zhang, "Security Research in Personnel Electronic File Management Based on Blockchain Technology," *Security and Communication Networks*, vol. 2022, Article ID 7875825, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7875825, 8 pages
https://doi.org/10.1155/2022/7875825

Research Article

Security Research in Personnel Electronic File Management Based on Blockchain Technology

Hongbing Wang [1] **and Jian Zhang** [2]

[1]*Personnel, Wuxi Vocational College of Science and Technology, Wuxi 214101, China*
[2]*College of Artificial Intelligence, Wuxi Vocational College of Science and Technology, Wuxi 214101, China*

Correspondence should be addressed to Jian Zhang; 2016009@wxsc.edu.cn

Received 4 June 2022; Revised 21 June 2022; Accepted 5 July 2022; Published 30 July 2022

Academic Editor: Hangjun Che

Compared with traditional files, electronic personnel files have the characteristics of the economy, environmental protection, convenience, and sharing and are gradually replacing traditional paper files. However, the development of electronic archives is still in its infancy, and there are still many problems, including the professional quality of personnel, information management, and the security of electronic archives storage. As an emerging technology, blockchain technology has the characteristics of decentralization, immutability, and traceability. This paper applies blockchain technology in the management of electronic archives, overcomes the internal distortion and insecurity of electronic archives, and designs an electronic archives management module based on blockchain technology. Through the application in some schools, the effectiveness and practicability of the algorithm are proved.

1. Introduction

With the continuous popularization and maturity of big data, cloud computing, and blockchain technology, traditional archives can no longer meet the development needs of employers. Therefore, promoting the electronic management of personnel files is an inevitable trend of informatization development of employers [1]. Electronic archives are an important form of archives digital management. They are archived information stored on specific media using computer technology and are also an important means of archiving modern management [2]. Compared with traditional files, electronic personnel files have the characteristics of the economy, environmental protection, convenience, and sharing [3]. The superiority of personnel electronic file management in file information inquiry, storage, and processing is unmatched by traditional file management. However, the development of electronic archives is still in its infancy, and there are still many problems, including the professional quality of personnel, information management, the security of electronic archives storage equipment, the security of the network, the security of stored information, and so on [4–6].

As an emerging technology in recent years, blockchain technology has the characteristics of decentralization, immutability, traceability, openness, and transparency [7, 8]. There have been some attempts in many fields, including finance, logistics, Internet of Things, public services, copyright, and so on. Its security features can also be applied to electronic file management to improve the efficiency and safety of the entire electronic file management [9]. This article will analyze the problems in electronic file management and apply blockchain technology to solve many existing problems.

2. Electronic File Management and Blockchain Technology

2.1. Advantages and Problems of Electronic Archives. Compared with traditional paper archives, electronic archives have obvious advantages [10], which are mainly reflected in the following points:

(1) *Electronic Files Can Reduce Operating Costs* [11]. In the file management of the personnel system, electronic files can reduce the operating cost of the employer. Traditional personnel file statistics, sorting, and querying require more labor costs. At the same time, it needs to invest a lot of economic costs such as copying, printing, binding, and mailing. In addition, paper files need to be kept, and hardware costs such as fire and moisture resistance are required. The management of electronic records can greatly reduce these operating costs [12–14].

(2) *Electronic File Management Is Shared*. Limited by time and place, traditional paper archives also have certain limitations [15]. In particular, paper archives are usually only used by one person and cannot share information resources, which greatly limits the exchange of information. Electronic archives management breaks this limitation and can realize the sharing of archives resources. Realize the interconnection of file resources, allowing employees to complete data sharing in real time. Big data is massive, diverse, real-time, and valuable, providing strong support for the sharing of electronic archives resources, and comprehensively improving the service quality and capabilities of archives [16–19].

(3) *The Management of Electronic Files Is Relatively Easy* [20]. The files include personal academic certificates, professional title materials, salary, job transfer, social relations, and other information. These electronic documents can be named according to certain rules to facilitate searching, updating, and other operations. At the same time, the formulation of rules and systems is relatively easy and easier to manage [21].

Despite the advantages of electronic records, there are also many problems.

(1) The management system is not perfect, and the construction of the personnel team is lagging behind [22]. Because the management of electronic archives in colleges and universities covers the whole process of the life cycle of electronic documents, it involves a wide range of areas and has many contents, so the original archives management system and management system are not suitable. For example, the creation, circulation, inspection, and utilization of electronic files lack specific rules and regulations, resulting in management loopholes and inadequacies. There are unreasonable structures and unstable personnel in the construction of electronic archives management teams in colleges and universities. Such as the majority of the full-time file management personnel are the elderly, the ability to update knowledge and accept new things is slow, and the young are enthusiastic but unwilling to engage in this boring work [23, 24].

(2) It is easy to be distorted in electronic files. Compared with paper archives information, the content of digital archives information is easier to be artificially forged, tampered with, and deleted without leaving traces [25]. The reasons include digital archives information can be stored on various carriers, managers and users can read and artificially modify digital archives information with various devices without leaving traces; due to inconsistent operating systems or software versions, it is prone to distortion problems such as unrecognized digital archive information and image distortion; the current digital archive information management system is mainly based on centralized nodes, databases, and servers. The operation of the system depends on the operations of various managers. Once the digital file information is artificially tampered with, the wrong digital file information will flow into the entire system, causing damage to the authenticity of the digital file information [26].

(3) Insecurity of storage hardware and network. Electronic files are stored on hard disks, servers, and other hardware. Usually, these devices are connected to the Internet, which poses a security risk. Cyberattacks, hacker attacks, and insider attacks may all be potential threats. These are all centralized devices or servers with relatively high risks [27].

Blockchain technology has the characteristics of decentralization, nontampering, traceability, openness, and transparency, which can reduce these security risks to a certain extent.

2.2. Blockchain Technology. Blockchain technology is the underlying technology of Bitcoin. Although there are many international disputes in digital currencies such as Bitcoin, it is undeniable that blockchain technology is being used more and more in finance, logistics, notarization, and many other industries [28]. The so-called blockchain is to store data in blocks and then connects all blocks insequence and links themtogether, as shown in Figure 1.

Blockchain technology has the following characteristics:

(1) *Decentralization*. The so-called decentralization refers to the use of several nodes composed of blockchain technology to form a database, which is relatively complete, closed, and does not have a centrally managed organization or equipment [29]. As shown in Figure 2, Figure 2(a) is a centralized structure, with a central server, and other nodes store data in the centralized server. If the data in the centralized server is distorted, the entire information will be distorted. Figure 2(b) is decentralized. There is no centralized server. All devices are part of the server. Even if the data of some machines is lost, they can be recovered by other machines.

(2) *Detrust*. Blockchain technology uses a set of transparent and open encryption algorithms to enable the exchange of data and information at all stages of the system under sufficient trustless conditions. Under the conditions of the blockchain network, each network-connected device acts as an independent

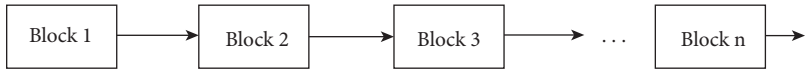


Figure 1: Chain structure.

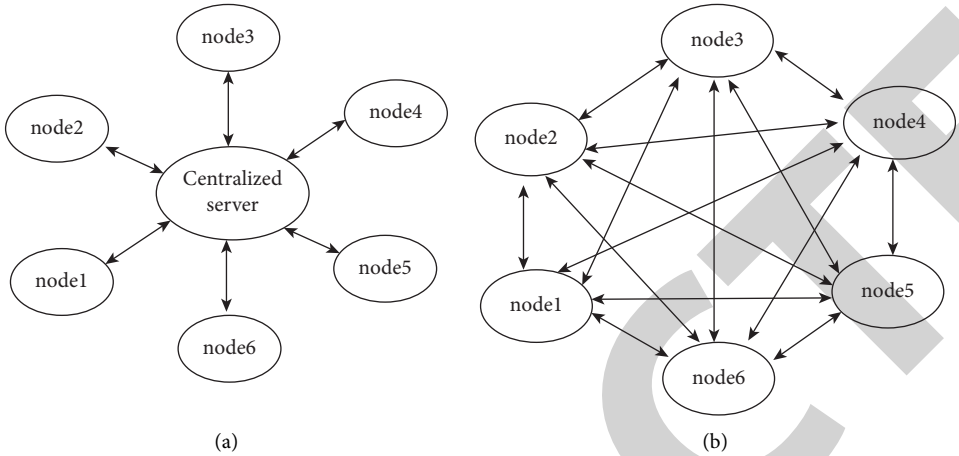


Figure 2: The difference between centralization and decentralization. (a) Centralized Node (b) Decentralized Node.

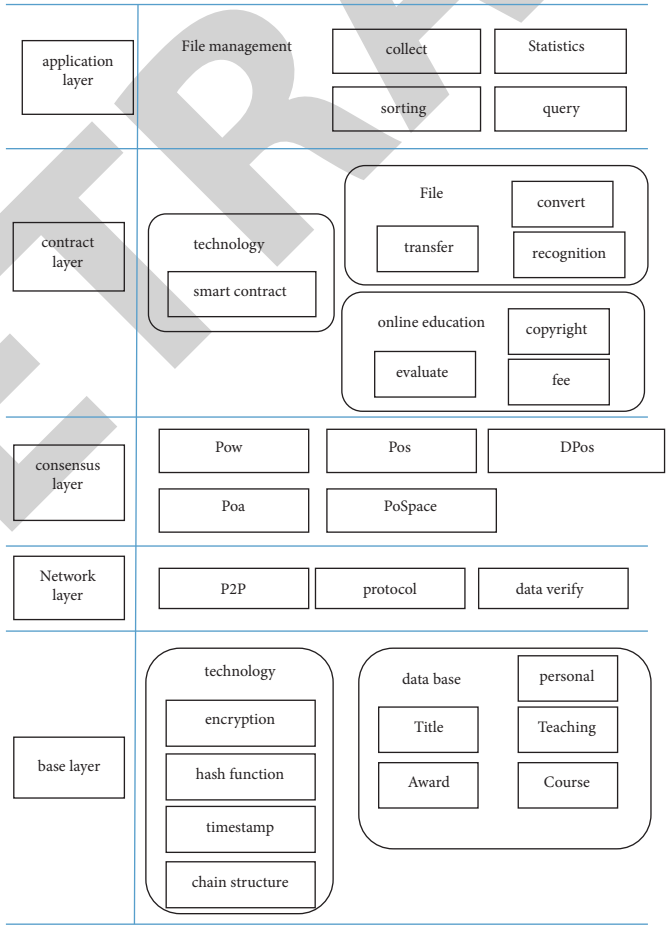


Figure 3: Electronic file management system based on blockchain technology.

node, based on a consensus protocol or specification, automatically and securely exchanges data without trust, and both parties do not need to disclose each other's identities.

(3) *Traceability*. Blockchain technology relies on time stamps and sequential results, which can not only accurately record the creation time of file information in the database but also trace the information of all blocks. The decentralized structure makes the wrong information of any node will not affect the results of the entire network, and the traceability of information is strong.

(4) *Strong security*. Many cryptographic algorithms are applied in the blockchain system, which can effectively keep the stored information confidential. In addition, the application of the hash algorithm can ensure that the information in the database is not tampered with, the information is kept confidential and secure, and the antitampering function is outstanding.

3. Security Design of Electronic Archives Management Based on Blockchain Technology

Using the decentralization, traceability, and encryption algorithm design in the characteristics of blockchain, an electronic file management system based on blockchain technology is designed, as shown in Figure 3. The electronic file management system includes five layers, namely, the base layer, the network layer, the consensus layer, the contract layer, and the application layer. The basic layer includes some underlying technologies and basic data; the network layer includes P2P and other protocols; the consensus layer is some consensus algorithms; the contract layer is some smart contract algorithm technologies; the application layer is the management layer of electronic files, including operations such as collection and processing.

In this structure, each layer involves security, including the underlying hash algorithm and encryption algorithm; the security protocol of the network layer; the security architecture of the consensus layer; the intelligent encryption of the contract layer; the data storage of the application layer, etc. This article will analyze the security of the hash algorithm, the security design of the alliance chain, the security design of data sharing, the security design of the electronic archives platform, and the security encryption algorithm design of electronic archives storage.

3.1. Security of Hash Algorithm. The Hash algorithm is a method of creating small numbers from arbitrary files. Like a fingerprint, a hash algorithm is a sign that guarantees the uniqueness of a file with a short piece of information. This sign is related to every byte of the file, and it is difficult to find a reverse pattern. Therefore, when the original file changes, its flag value will also change, thus telling the file user that the current file is not the file you need.

The Hash algorithm can map binary plaintexts of arbitrary length into shorter binary strings, and it is difficult for different plaintexts to be mapped to the same Hash value.

Hash values have the following characteristics:

Forward fast: given the plaintext and Hash algorithm, the hash value can be calculated in limited time and limited resources

Reverse difficulty: given the hash value, it is difficult to reverse the plaintext in a finite time

Input sensitivity: any change in the original input information, the new Hash value should change greatly

Collision avoidance: it is difficult to find two pieces of plaintext with different contents so that their hash values are the same

The Hash algorithm includes many logical functions, as shown in the following equations:

$$Ch(x, y, z) = (x \wedge y) \oplus (x \wedge z), \tag{1}$$

$$Ma(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z), \tag{2}$$

$$\sum_{0} x = S^{2}(x) \oplus S^{13}(x) \oplus S^{22}(x). \tag{3}$$

3.2. Security Design of Consortium Chain. Blockchain can be divided into the public chain, alliance chain, and private chain. The public chain means that anyone can participate in the use and maintenance, such as the Bitcoin blockchain, and the information is completely open. The public chain is completely decentralized, and anyone can participate in the consensus process. The private chain emphasizes privacy; that is, the writing authority is in the hands of an organization and unit, which is centrally controlled by the organization, but different distributions and branches are decentralized and collaborative. The alliance chain is a system form between the public chain and the private chain, which is often controlled by multiple centers. Several organizations work together to maintain a blockchain, the use of which must be restricted access with permissions, and the relevant information will be protected.

Because university archives data is generally circulated among personnel departments, educational affairs departments, science and technology departments, party and mass departments, scientific research institutes, and universities, it not only breaks through the geographical restrictions of institutions but also eliminates the free participation of all groups, which is more similar to the application scenario of the alliance chain fit. Therefore, this paper proposes a consortium chain architecture that allows stakeholders to join the consortium system conditionally, and the file data are open to the nodes in the chain, but the permissions of each node will be different. For example, the personnel department, educational affairs department, and scientific research management department of archives management are trusted nodes and have certain operating authority. On-campus party and mass departments, teaching departments,

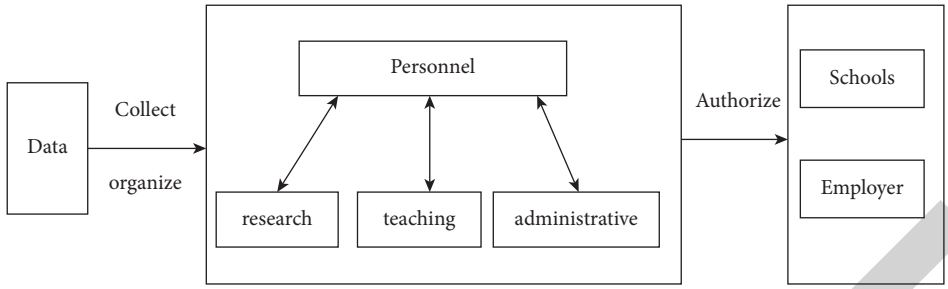


Figure 4: Alliance chain.

Table 1: Time test.

Process	Time tes t(s)- electronic file 1	Time tes t(s)- electronic file 2
Blinded	0.7	0.65
Blind signature	0.12	0.13
Verify	0.1	0.15

and off-campus education departments, science and technology departments, and scientific research institutes are participating nodes. A trusted node is required to authenticate and authorize it.

The security architecture of the electronic archives alliance chain is shown in Figure 4. Each department is responsible for collecting data and summarizing it to the personnel department. These departments can read data according to permissions. Relevant schools and enterprises can apply and read the data after obtaining authorization.

3.3. Identity-Based Blind Signature Scheme. Elliptic Curve Cryptosystem (ECC) is an efficient cryptosystem based on the intractability of the elliptic curve discrete logarithm problem. It can achieve the same security level as the RSA encryption algorithm and the discrete logarithm system with a shorter number of operations. Compared with other public key algorithm systems, ECC has obvious performance advantages in terms of bandwidth and complexity and is very suitable for blockchain related modules.

Identity-based blind signature schemes include key generation, signing, and verification.

The signer generates a private key S_I and sends S_I to the signer through a secure channel. The signer is verified according to the following formula:

$$S_I G - Q_I P = \begin{Bmatrix} 0 & \text{TRUE}, \\ 1 & \text{FALSE}. \end{Bmatrix}. \tag{4}$$

In which, G is the n-order base point on the elliptic curve, Q_I is the Hash function, and P is the public key. If the verification is 0, it is true, indicating that the key generation is successful.

The signer calculates the public key R and sends it to the user. The user generates factors β, γ, and δ to obtain the elliptic curve equation.

$$R + \beta G + \gamma H + \delta Q = (X, Y). \tag{5}$$

After blinding, e is obtained, and e is signed and verified.

$$e = M(mx(\mathrm{mod}p)I) - \delta. \tag{6}$$

The data in Table 1 was obtained by testing different archive sets.

3.4. Security Design of Data Sharing. The data sharing mechanism of electronic archives can be realized through smart contracts. A smart contract is a simple transaction that can be executed automatically. It is stored in the blockchain and synchronized between nodes to maintain the consistency of the contract. A full self-service file service system based on blockchain technology can first formulate smart contracts and then spread them into each node. After the file user enters personal information and usage requirements, the system automatically executes according to the preset method when the corresponding conditions of a certain mechanism are met, as shown in Figure 5. Both the data application and the printing application need to be reviewed, judged, and automatically executed by the smart contract and finally authorized to the user.

3.5. Security Design of Electronic Archives Platform. The framework of the blockchain-based electronic archives platform is shown in Figure 6. The platform includes a blockchain recording platform, a blockchain security platform, a blockchain scheduling platform, a blockchain hardware platform, and a node management platform. Through these platforms, data access, access control, traceability management, judgment, and payment are realized. The blockchain security platform is responsible for the security of the entire structure.

3.6. Design of Secure Encryption Algorithm for Electronic File Storage. In the personnel file information, there is a lot of picture information that needs to be encrypted and stored. In a blockchain network, storage is an important content and can be stored in multiple nodes. For privacy, images need to be encrypted and saved. There are many encryption

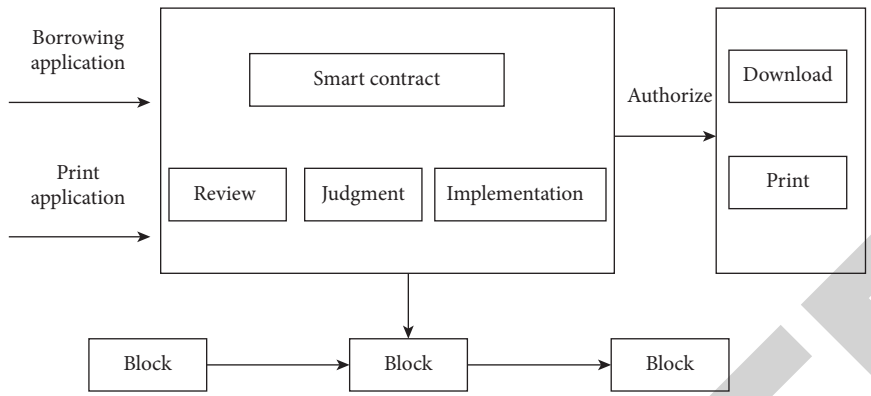


Figure 5: Smart contract.

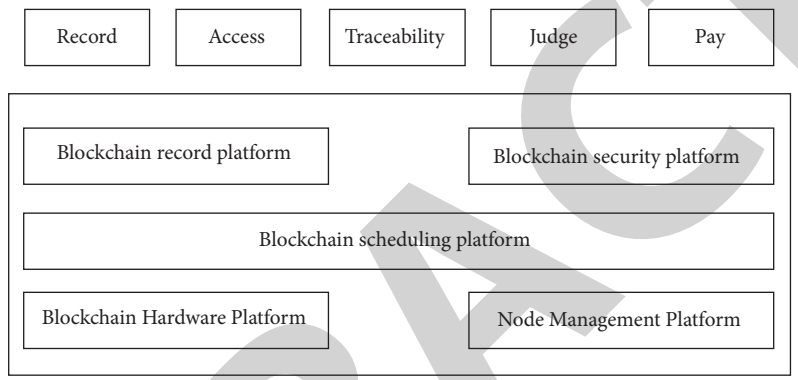


Figure 6: Blockchain platform.

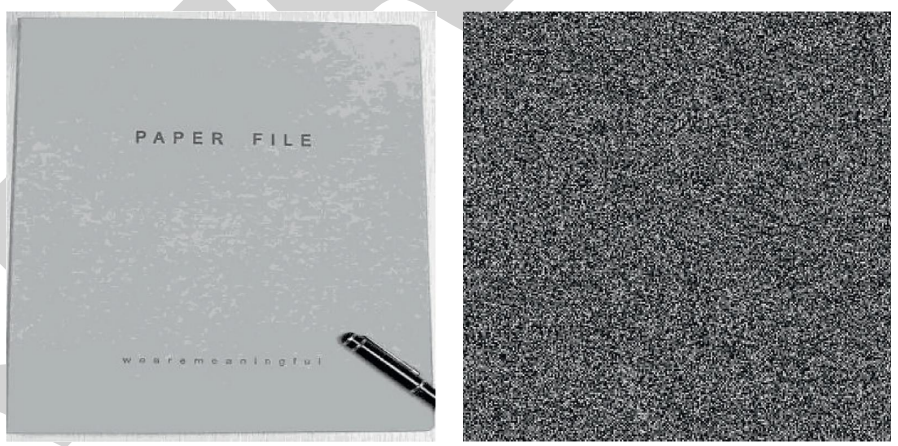


Figure 7: The image encryption algorithm.(a) original image (b) encrypted image.

algorithms to choose from, this paper proposes a fast image encryption algorithm.

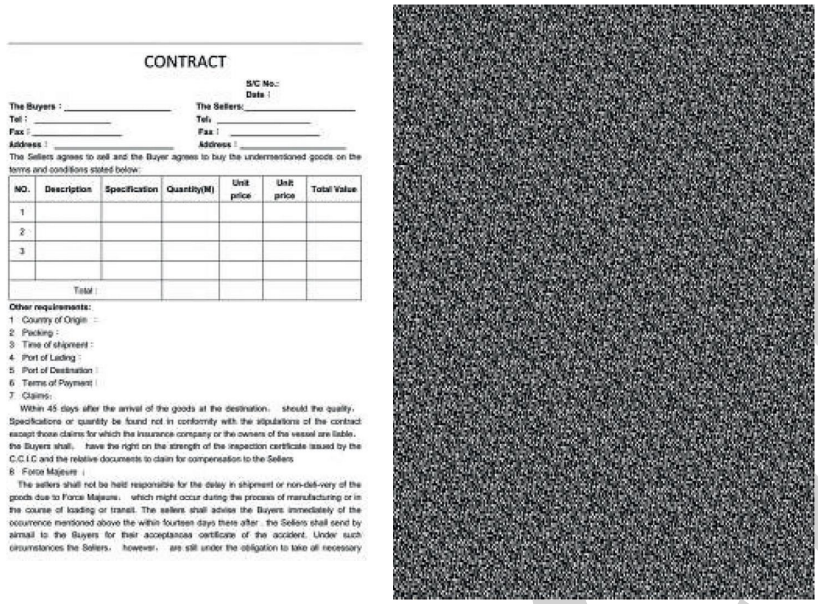
Arnold cat transformation is a classic position mapping transformation, and its expression is shown in the following equation (4):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (N). \tag{7}$$

Here, x_n, y_n is the original pixel position of an $N \times N$ image, x_{n+1}, y_{n+1} is the scrambled pixel position, a and b are system parameters, take positive integers, when $a = 1, b = 1$, it is the standard Arnold cat transformation.

The pixel value scrambling is performed by the spread function, and its expression is shown in formula (5).

$$v_k' = v_k + Z^2 \bmod 256., \tag{8}$$


CONTRACT

S/C No.:
Date :

The Buyers : _____ The Sellers: _____
Tel : _____ Tel: _____
Fax : _____ Fax : _____
Address : _____ Address : _____

The Sellers agrees to sell and the Buyer agrees to buy the undermentioned goods on the terms and conditions stated below:

NO.	Description	Specification	Quantity(M)	Unit price	Unit price	Total Value
1						
2						
3						
	Total :					

Other requirements:
1 Country of Origin :
2 Packing :
3 Time of shipment :
4 Port of Lading :
5 Port of Destination :
6 Terms of Payment :
7 Claims:
Within 45 days after the arrival of the goods at the destination, should the quality, Specifications or quantity be found not in conformity with the stipulations of the contract except those claims for which the insurance company or the owners of the vessel are liable, the Buyers shall, have the right on the strength of the inspection certificate issued by the C.C.I.C and the relative documents to claim for compensation to the Sellers
8 Force Majeure :
The sellers shall not be held responsible for the delay in shipment or non-delivery of the goods due to Force Majeure, which might occur during the process of manufacturing or in the course of loading or transit. The sellers shall advise the Buyers immediately of the occurrence mentioned above the within fourteen days there after. the Sellers shall send by airmail to the Buyers for their acceptances certificate of the accident. Under such circumstances the Sellers, however, are still under the obligation to take all necessary

(a) (b)

Figure 8: The image encryption algorithm (a) original image (b) encrypted image.

The encrypted storage of images can be realized by formulas (1) and (2). Figure 7(a) is the original image that needs to be saved. After encryption, the encryption effect is shown in Figure 7(b) is obtained. Figure 8(a) is the original image that needs to be saved. It can be seen that the encrypted image has no original information and is a messy picture. When decrypting, only the correct key can be recovered, so it can play the role of image privacy protection.

4. Conclusion

By analyzing the advantages and problems of electronic archives, its security is one of the problems that need to be solved. Some security features of blockchain technology can solve this problem very well. This paper designs an electronic file management system based on blockchain technology, from the security of hash algorithm, the security of alliance chain, the security of data sharing, the security of electronic file platform, and the security encryption algorithm of electronic file storage. Applied in some departments, it has already produced a positive effect.

Data Availability

The simulation experiment data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the 2021 Jiangsu Provincial Library Big Data Research Project of China (Grant no. 2021JSTD021).

References

[1] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," in *Public-Key Cryptography – PKC 2013*, K. Kurosawa and G. Hanaoka, Eds., Vol. 125–142, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[2] M. F. Leung and J. Wang, "Minimax and bi-objective portfolio selection based on collaborative neurodynamic optimization," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 7, pp. 2825–2836, 2021.

[3] A. Girdhar and V. Kumar, "Comprehensive survey of 3D image steganography techniques," *IET Image Processing*, vol. 12, no. 1, pp. 1–10, 2018.

[4] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Processing*, vol. 164, no. 4, pp. 249–266, 2019.

[5] Z. Chen, X. Yuan, Y. Yuan, H. H. C. Iu, and T. Fernando, "Parameter identification of chaotic and hyper-chaotic systems using synchronization-based parameter observer," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 9, pp. 1464–1475, 2016.

[6] P. Kumar, N. Langberg, J. Oded, and K. Sivaramakrishnan, "Voluntary disclosure and strategic stock repurchases," *Journal of Accounting and Economics*, vol. 43, no. 2, pp. 111–121, 2017.

[7] Y. Sun, C. Xu, G. Li et al., "Intelligent human computer interaction based on non-redundant EMG signal," *Alexandria Engineering Journal*, vol. 59, no. 3, pp. 1149–1157, 2020.

[8] G. Li, L. Zhang, Y. Sun, and J. Kong, "Towards the sEMG hand: internet of things sensors and haptic feedback

application," *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 29765–29782, 2019.

[9] D. Jiang, G. Li, Y. Sun, J. Hu, J. Yun, and Y. Liu, "Manipulator grabbing position detection with information fusion of color image and depth image using deep learning," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 12, pp. 10809–10822, 2021.

[10] K. Yang, Y. Wei, S. Li, L. Liu, and L. Wang, "Global financial uncertainties and China's crude oil futures market: evidence from interday and intraday price dynamics," *Energy Economics*, vol. 96, no. 4, Article ID 105149, 2021.

[11] Y. Wei, L. Bai, K. Yang, and G. Wei, "Are industry- level indicators more helpful to forecast industrial stock volatility? Evidence from Chinese manufacturing purchasing managers index," *Journal of Forecasting*, vol. 40, no. 1, pp. 17–39, 2020.

[12] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, 2021.

[13] L. Rivoirard, M. Wahl, and P. Sondi, "Multipoint relaying versus chain-branch-leaf clustering performance in optimized link state routing-based vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 1034–1043, 2020.

[14] S. S. S. Kumar, M. J. L. Iqbal, J. S. Sujin, R. Sowmya, and S. D. Kumar, "Recent advancements in automation to enhance vehicle technology for human centred interactions," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 2, pp. 550–556, 2019.

[15] C. Rus, R. Marcus, L. Pellegrini, M. Leba, M. Rebrisoreanu, and A. Constandoiu, "Electric cars as environmental monitoring IoT Network," in *Proceedings of the IOP Conference Series: Materials Science and Engineering*, IOP Publishing, Iasi, Romania, May 2019.

[16] H. Seliem, R. Shahidi, M. H. Ahmed, and M. S. Shehata, "Drone-based highway-VANET and DAS service," *IEEE Access*, vol. 6, 20137 pages, 2018.

[17] G. Shah, R. Valiente, N. Gupta et al., "Real-time hardware-in-the-loop emulation framework for DSRC-based connected vehicle applications," 2019, https://arxiv.org/abs/1905.09267.

[18] U. Shaikh and N. Thalkar, "Vehicle communication systems: technology and review," in *Proceedings of the Conference on Technologies for Future Cities (CTFC)*, Mumbai, Maharashtra, March 2019.

[19] S. A. Ahmad, A. Hajisami, H. Krishnan, F. Ahmed-Zaid, and E. Moradi-Pari, "V2V system congestion control validation and performance," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2102–2110, 2019.

[20] P. Sewalkar and J. Seitz, "Vehicle-to-pedestrian communication for vulnerable road users: survey, design considerations, and challenges," *Sensors*, vol. 19, no. 2, p. 358, 2019.

[21] Q. Jiang, F. Shao, W. Lin, K. Gu, G. Jiang, and H. Sun, "Optimizing multistage discriminative dictionaries for blind image quality assessment," *IEEE Transactions on Multimedia*, vol. 20, no. 8, pp. 2035–2048, 2018.

[22] S. Qu, W. Xu, J. Zhao, and H. Zhang, "Design and implementation of a fast sliding-mode speed controller with disturbance compensation for SPMSM syste," *IEEE Transactions on Transportation Electrification*, vol. 99, p. 1, 2021.

[23] Z. Wu, A. Song, J. Cao, J. Luo, and L. Zhang, "Efficiently translating complex SQL query to mapreduce jobflow on cloud," *IEEE transactions on cloud computing*, vol. 8, no. 2, pp. 508–517, 2020.

[24] N. Xiao, R. Xinyi, Z. Xiong et al., "A diversity-based selfish node detection algorithm for socially aware networking," *Journal of Signal Processing Systems*, vol. 93, no. 7, pp. 811–825, 2021.

[25] P. Wang, "Research and practice of book recommendation system based on SNS," *Computer Applications and Software*, vol. 29, no. 12, pp. 21–23, 2012.

[26] G. Wang, "Recommendation algorithm for E-learning resources based on improved collaborative filtering," *Journal of Chinese Computer Systems*, vol. 42, no. 5, pp. 940–945, 2021.

[27] C. Liu, "Collaborative filtering hybrid recommendation algorithm based on improved biased and cluster user nearest neighbor," *Computer Applications and Software*, vol. 38, no. 5, pp. 288–293, 2021.

[28] M. F. Leung and J. Wang, "A collaborative neurodynamic approach to multiobjective optimization," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 11, pp. 5738–5748, 2018.

[29] M. C. Yuen, S. C. Ng, and M. F. Leung, "A competitive mechanism multi-objective particle swarm optimization algorithm and its application to signalized traffic problem," *Cybernetics & Systems*, vol. 52, no. 1, pp. 73–104, 2021.