International Journal for Housing Science and Its Applications
Publish August 6, 2025. Volume 46, Issue 3 Pages 9013-9017

https,//doi.org/10.70517/ijhsa463772

Analysis of the Impact of Blockchain-Enabled Shareholder Voting Systems on Corporate Governance

Zongpeng Xu[1,*]
[1] Anshan Normal University, Anshan, Liaoning, 114000, China
Corresponding authors: (e-mail: asxuzongpeng@163.com).

Abstract This paper presented the technology of intelligent contracts as a means of achieving transparency in information data. An intelligent contract can enable data transfer transparency and traceability, automatically adhere to predetermined criteria, and provide better control and transparency over the data transmission and storage process. The study used the Enron Email Dataset to confirm that the suggested approach works as intended. This paradigm offered a number of advantages over conventional digital signature techniques like RSA. This approach enhanced data transmission integrity and transparency while guaranteeing the security and dependability of information transfer and storage.

Index Terms Information Data Flow, Risk of Data Tampering, Information Transparency, Blockchain Technology, Smart Contract Technology

I. Introduction

In today's digital information environments, seamless data flow and sharing are crucial across many different sectors [1]. However, there are a number of disadvantages to conventional data flow methods, such as a lack of transparency [2] and the potential for manipulation [3].

Research has examined digital signature algorithms, particularly the RSA method, to verify the validity and integrity of data [4]. In particular, Badawy M's research demonstrates the level of security achievable for Internet of Things (IoT) networks and investigates the possibility of using RSA as a stream key generator [5], [6].

The immutability of blockchain technology may help to assure data integrity and authenticity [7], [8]. Researchers such as Zhaofeng M, who have studied the application of these approaches to address trust and security concerns in the management of enormous data from the Internet of Things, have proposed a blockchain-based decentralized trust management approach for IoT big data licensing [9]. Additionally, this study highlighted smart contract technology as a revolutionary element that generates enforceable policies and guidelines that support the traceability and openness of information data. The practical application of this approach is exemplified in Yang X's suggestion of a blockchain-based traceability system for storing and retrieving product data in the agricultural supply chain [10].

II. Construction of Information Data Flow Verification Model

II. A.Blockchain Technology

Blockchain technology is a distributed database technology [11]. The implementation process is shown in formula 1.

$$\mathrm{Block}_{\mathrm{current}} = \mathrm{H}(\mathrm{Data} + \mathrm{Previous\_Hash}) \tag{1}$$

Here, $\mathrm{Block}_{\mathrm{current}}$ is the hash value of the current block, $\mathrm{H}()$ is a hash function, Data is the data stored in the block, and $\mathrm{Previous\_Hash}$ is the hash value of the previous block. In this way, each block contains the hash value of the previous block, forming a chain structure. Due to the immutability of the blockchain, any tampering with stored data can cause the consistency of the blockchain to be compromised, making it detectable. In addition, the distributed storage characteristics of blockchain can be utilized to ensure the reliability of data. Data is stored in a distributed manner on multiple nodes in a blockchain network, rather than being centrally stored on a single centralized server. This distributed storage method can be represented by formula 2.

$$\mathrm{Storage\_Node\_i} = \frac{1}{\mathrm{N}} \times \mathrm{Total\_Data} \tag{2}$$

Among them, $Storage\_Node\_i$ represents the amount of data stored by the i-th node, N is the number of nodes in the grid, and $Total\_Data$ is the total amount of data in the system. This distributed storage method increases data redundancy, improves system reliability and resistance to attacks. Even if one node fails or is attacked, other nodes can still provide normal services, ensuring data reliability.

II. B.Smart Contracts Achieve Information Transparency

Smart contracts are based on blockchain based automated computer programs that can execute pre encoded logic without the need for third-party intervention. In the flow of information data, smart contracts can ensure the transparency, integrity, and traceability of data transmission. Firstly, the smart contract ensures the compliance of data transmission by executing specific verification rules. A data transmission rule R is set, and during the transmission process, the smart contract can verify whether the transmitted data complies with the rules through condition formula 3.

$$\text{if Condition=R: Transfer\_Data} \tag{3}$$

Among them, $Condition$ is the agreed rule condition. If the transmission rule R is met, the data can be transmitted according to $Transfer\_Data$'s requirements. Secondly, to ensure transparency in data transmission, smart contracts record detailed information for each transmission, including the sender, receiver, and the content of the transmitted data.

$$Transaction\_Record = Sender + Receiver + Data \tag{4}$$

The implementation process is shown in formula 5.

$$Contract\_Log = Action\_Log + Execution\_Result \tag{5}$$

Among them, $Contract\_Log$ is the log record of the smart contract, which includes all operations and results during the execution of the smart contract; $Action\_Log$ is the log of specific actions or operations recorded during the execution of the smart contract, which includes every operation that occurs in the contract. $Execution\_Result$ is the result record of smart contract execution, which records the final result or status of the smart contract during the execution process. This recording method makes the system's operations and results auditable, and any results and related operations of contract execution can be audited and traced.

III. Model Evaluation

III. A. Experimental Setup

(1) Experimental environment configuration

The operating environment for this experiment is the Ubuntu 20.04 LTS operating system, running on the Intel Core i7-8700 processor (3.70GHz) and equipped with 16GB of memory. It adopts Ethereum as the blockchain platform, and the development language for smart contracts is Solidity. Remix ID is used as the programming tool for writing and deploying smart contracts for model training and evaluation.

(2) Dataset selection

This article selected Enron Email Dataset as the main dataset for this experiment, which includes 100000 types of data such as emails and documents. Each data record includes fields such as sender, receiver, email content, and timestamp.

III. B. Experimental Results

III. B. 1) Data Integrity Verification Experiment

5000 data records were chosen at random for data integrity verification from the Enron Email Dataset dataset, which consists of two categories of information data: email data and document data. Table 1 displays the recall, accuracy, and precision numbers for each algorithm model for this example data in this research. The statistics in Table 1 are examined in this article. The system model has obtained good accuracy, recall, and precision scores, ranging from 0.91 to 0.97, for both email and document data types. The accuracy, recall, and precision of the conventional algorithm models—RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital Signature Algorithm)—range from 0.68 to 0.91, indicating poorer performance.

Table 1: Comparison of data integrity validation results between the paper's system model and traditional algorithms

Model	Data type	Accuracy	Recall	Precision
The system model of this article	Email data	0.93	0.91	0.95
The system model of this article	Document data	0.96	0.95	0.97
RSA	Email data	0.88	0.86	0.90
RSA	Document data	0.89	0.88	0.91
DSA	Email data	0.70	0.68	0.72
DSA	Document data	0.75	0.73	0.77
ECDSA	Email data	0.82	0.80	0.84
ECDSA	Document data	0.84	0.82	0.86

This research computed the average accuracy, recall, and precision of each algorithm model for these two data kinds in order to observe the performance of the system model in data integrity verification more intuitively in comparison to standard algorithm models (RSA, DSA, and ECDSA). Figure 1 displays the results of the calculation. It is evident from the data in Figure 1 that the system model exhibits the highest average accuracy of 0.945 for the average accuracy. The paper's system model outperforms other standard algorithm models in data integrity verification, as evidenced by the lower average accuracy of RSA, DSA, and ECDSA, which are 0.885, 0.725, and 0.83, respectively.

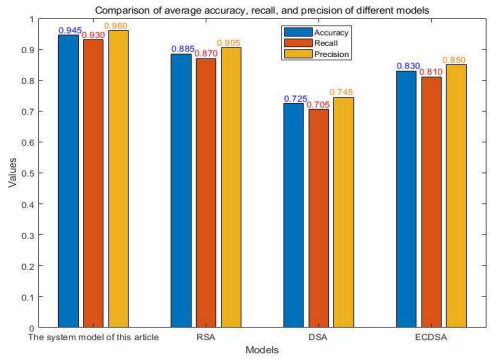

Figure 1: Comparison of average accuracy, recall, and accuracy of different models

III. B. 2) Comparative Experiment on Transparency and Auditability of Information Transmission

Transparency and auditability were utilized as evaluation indicators in this experiment to assess the information transmission's transparency and auditability in this system paradigm. This work acquired the evaluation index results of each model by contrasting the performance of the system model with traditional algorithm models (RSA, DSA, and ECDSA) on various sample data kinds, as indicated in Table 2. Table 2's third column displays each model's information transmission transparency for various data kinds, including email and document data. Compared with other conventional models, this system model has substantially greater transparency values, with email data and document data having transparency values of 93% and 95%, respectively.

Table 2: Comparative experimental results of information transmission transparency and auditability

Model	Data type	Transparency	Audibility
The system model of this article	Email data	93%	92%
The system model of this article	Document data	95%	94%
RSA	Email data	85%	84%
RSA	Document data	88%	87%
DSA	Email data	72%	74%
DSA	Document data	75%	76%
ECDSA	Email data	81%	83%
ECDSA	Document data	82%	84%

Next, in order to evaluate the comprehensive performance of the paper's system model in terms of information transmission transparency and auditability for different data types, this paper calculated the average transparency and auditability evaluation indicators of each algorithm model for these two data types (email data and document data). After calculation, the average transparency and auditability values of the system model are 94% and 93%, respectively. The average transparency and auditability values of the RSA traditional algorithm model are 86.5% and 85.5%, respectively, while the average transparency and auditability values of the DSA traditional algorithm model are 73.5% and 75%, respectively. The average transparency and auditability values of the traditional ECDSA algorithm model are 81.5% and 83.5%, respectively. This article can plot these data as shown in Figure 2. From Figure 2, it can be intuitively seen that the system model has the highest average transparency value and average auditability value (94%, 93%) compared to other traditional algorithm models. Compared to the traditional RSA algorithm model, it has increased the average transparency value and average auditability value by 7.5%. These data demonstrate that the system model performs the best in terms of transparency and auditability in information transmission when facing different data types. It is not affected by the data type.

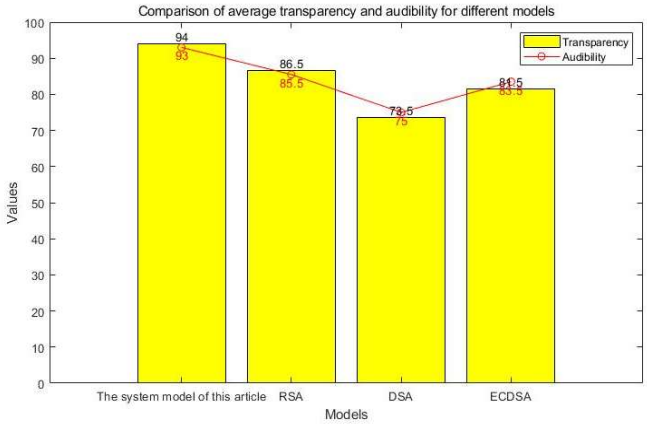

Figure 2: Comparison of average transparency and auditability among different models

IV. Conclusions

This article constructed a blockchain based information data flow verification model to effectively address the risks of data tampering and insufficient transparency in traditional data flow. In order to verify the performance of the system model, a comparative analysis was conducted with traditional algorithms in terms of data integrity verification, information transmission transparency, and auditability. The experimental results show that the system model exhibits higher accuracy, recall, and precision in data integrity verification. In terms of information transmission transparency and auditability, this system model provides a higher level of transparency and auditability. However, further consideration is needed in this study regarding dataset size, security, and the scalability of the model in practical scenarios. Future research directions include optimizing model performance, improving system security, and applying the model to a wider range of practical application scenarios.

Funding

This work was supported by the Project of Anshan Normal University (China) (under Grant 23kyxm069).

References

[1] Szymkowiak A, Melovic B, Dabic M, Jeganathan K, Kundi G S. Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people[J]. Technology in Society, 2021, 65: 101565.

[2] Yang J, Wen J, Jiang B, Wang H. Blockchain-based sharing and tamper-proof framework of big data networking[J]. IEEE Network, 2020, 34(4): 62-67.

[3] Cao Y, Jia F, Manogaran G. Efficient traceability systems of steel products using blockchain-based industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 16(9): 6004-6012.

[4] Chandrashekhara J, Anu V B, Prabhavathi H, Ramya B R. A comprehensive study on digital signature[J]. International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN, 2021: 2347-5552.

[5] Badawy M. Security Evaluation of Different Hashing Functions with RSA for Digital Signature[J]. IJCI. International Journal of Computers and Information, 2023, 10(2): 99-116.

[6] Al_Barazanchi I, Shawkat S A, Hameed M H, Al-Badri K S L. Modified RSA-based algorithm: A double secure approach[J]. TELKOMNIKA (Telecommunication Computing Electronics and Control), 2019, 17(6): 2818-2825.

[7] Politou E, Casino F, Alepis E, Patsakis C. Blockchain mutability: Challenges and proposed solutions[J]. IEEE Transactions on Emerging Topics in Computing, 2019, 9(4): 1972-1986.
[8] Wang S, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. Ieee Access, 2018, 6: 38437-38450.
[9] Zhaofeng M, Lingyun W, Aochang W, Zhen W, Weizhe Z. Blockchain-enabled decentralized trust management and secure usage control of IoT big data[J]. IEEE Internet of Things Journal, 2019, 7(5): 4000-4015.
[10] Yang X, Li M, Yu H, Wang M, Xu D, Sun C. A trusted blockchain-based traceability system for fruit and vegetable agricultural products[J]. IEEE Access, 2021, 9: 36282-36293.
[11] Shao Qifeng, Zhang Zhao, Zhu Yanchao, Zhou Aoying. Summary of enterprise-level blockchain technology [J]. Journal of Software, 2019, 30(9): 2571-2592.