JIEM : JOURNAL INFORMATIC, EDUCATION AND MANAGEMENT
Vol. 5, No. 1, February 2023, pp. 1 ~ 6
ISSN: 2716-0696, DOI: https://doi.org/10.61992/jiem.v5i1.54

Implementation Of Blockchain Technology in Improving Information System Security

Adi Ahmad

STMIK Indonesia Banda Aceh

Article Info

Article history:
Received 10 February 2023
Revised 12 February 2023
Accepted 13 February 2023

Keywords:
Blockchain Technology, Information Systems, Security, Transparency, Decentralisation.

ABSTRACT

The purpose of this research is to analyse the implementation of blockchain technology in improving information system security. The research method used is a literature study by collecting information from various relevant primary and secondary sources. The results of this study show that blockchain technology has strong potential to strengthen information system security through its unique characteristics, such as decentralisation, transparency, and high cryptographic security. While analysing various existing studies, it was found that by implementing blockchain technology in information systems, user satisfaction may increase due to better auditability. However, careful attention is also needed to the weaknesses and challenges associated with blockchain technology, such as scalability, efficiency, and privacy. In conclusion, the use of blockchain technology in information systems can provide significant benefits in improving security. However, comprehensive measures should be taken to address issues and adapt this technology to the specific context and existing regulations.

This is an open access article under the CC BY-SA license.

Corresponding Author:
Adi Ahmad | STMIK Indonesia Banda Aceh
Email: audiest@gmail.com

1. INTRODUCTION

Advances in information technology have introduced new challenges in maintaining the security of information systems. The ever-growing threat of cyberattacks and data breaches has encouraged researchers and practitioners to seek innovative and effective solutions to improve the level of security. One promising innovation is the implementation of blockchain technology in information systems [1].

Blockchain technology, which bases its philosophy on decentralisation, transparency, and cryptographic security, has attracted widespread interest as a potential solution in improving the security of information systems. At a conceptual level, blockchain technology can be seen

as a distributed and encrypted "digital ledger" that permanently stores transactions. By relying on consensus indirectly, blockchain reshapes the traditional paradigm of trust in centralised systems by ensuring data integrity that cannot be manipulated efficiently [2].
Several experts have agreed that the implementation of blockchain technology can provide a higher level of security compared to traditional infrastructure. Blockchain can provide all entitled participants with secure and transparent access to relevant data or information, while also protecting user privacy by utilising strong cryptographic techniques. However, experts also give mixed opinions on the challenges, such as scalability, efficiency, and privacy issues associated with the use of blockchain technology in information systems. These aspects are indeed critical in identifying the implementation gap between the concept and practical reality of blockchain in the context of real information systems.

In this balanced view, this research aims to analyse the implementation of blockchain technology in enhancing information system security. This will involve a thorough literature review to establish a solid theoretical foundation and bring in the diverse views of experienced experts in enhancing the general understanding of blockchain technology and its implications in the context of information systems. In this article, we introduce a theoretical framework that focuses on exploring the concept of blockchain technology, its underlying security principles, and potential possibilities in bringing about changes in existing security practices. Through in-depth analysis and synthesis of reliable and relevant literature, this research hopes to make a valuable contribution towards a better understanding of the possible benefits and limitations of blockchain technology implementation in enhancing information system security.

2. THEORETICAL BASIS

a. Blockchain Technology:

Blockchain technology can be explained as two main concepts: blocks and chains. Blockchain combines the power of mathematical programming with cryptographic security to create a distributed network where related entities can securely conduct transparent and monitored digital exchanges [2].

b. Information Security:

Information security plays an important role in ensuring the integrity, confidentiality, and availability of information systems. The foundational concept of information security involves the CIA framework: Confidentiality, Integrity, and Availability. Blockchain provides a high level of security due to its secure data structure and strong cryptographic techniques [3].

c. Decentralisation:

One of the key characteristics of blockchain technology is decentralisation. Decentralisation makes blockchain different from traditional central server-based architectures, where decisions and control are centred on a single authority. With decentralisation, the security of information systems can be improved as there is no central point that is vulnerable to attacks or malicious manipulation of data [4].

d. Transparency:

Blockchain provides a significant level of transparency as all transactions are permanently recorded in a distributed network that can be accessed by all eligible participants. The ability to publicly audit and verify these transactions increases trust among users and maintains accountability [5].

e. Cryptographic Algorithms:

Blockchain technology relies on cryptographic algorithms to help ensure the security of data and transactions. These include hashing functions that enable the conversion of data into unique hash values, as well as encryption algorithms that ensure the confidentiality of sensitive information during transit [6].

f. Understanding these theoretical foundations is important in implementing blockchain technology in the context of information systems to enhance security. In this research, careful interpretation and selection of appropriate theories will help achieve a more thorough understanding of the concept and potential of implementing blockchain technology in improving information system security.

3. RESEARCH METHODOLOGY

This research aims to analyse the implementation of blockchain technology in improving information system security. This research uses a literature study approach with the aim of collecting relevant information from various primary and secondary sources related to this topic. This approach was chosen to ensure this research has a solid and comprehensive theoretical foundation.

The development method used includes the implementation of the following stages:

a. Selection and identification of literature sources to be used in the research. Literature sources may include scientific journals, conferences, reference books, research reports, and other reliable sources of information.
b. Data collection through literature studies involves searching for articles, books, and publications related to the implementation of blockchain technology in improving information system security. The data collected included the basic concepts of blockchain technology, information security, decentralisation, transparency, and cryptographic techniques.
c. Selection and exploration of relevant and quality literature sources to complete the necessary theoretical framework. The data found will be analysed to create a holistic and accurate synthesis.
d. Data analysis is conducted by applying specific analytical methods to formulate key themes and findings from the collected literature. Comparison, contrast and integration of information will be used to develop a comprehensive theoretical foundation.
e. Data verification is conducted through critical appraisal and selection of high-quality literature appropriate to the research context. This data verification ensures the accuracy and validity of the information used in the research.

Through this research method, we hope to gain in-depth insight into the implementation of blockchain technology in enhancing information system security. By conducting a

comprehensive literature study, we were able to understand the current concepts and practices related to this topic, as well as identify the advantages, weaknesses, and challenges that need to be considered in implementing blockchain technology in the context of information systems.

4. RESULTS AND DISCUSSION

The results of this study show that the implementation of blockchain technology can have a positive impact on improving information system security. Through a comprehensive literature study analysis:

a. Increased Security:

The implementation of blockchain technology in information systems can increase the level of security. The unique characteristics of blockchain, such as decentralisation and cryptographic security, offer protection from attacks that could potentially disrupt information systems. With a distributed network structure, security can be enhanced as there is no single centralised point that is the main target [7].

b. Data Transparency and Integrity:

Blockchain technology also brings high transparency and data integrity to information systems. By using blockchain, all transactions and changes to data are permanently recorded and held in chained blocks. This allows for easy inspection and verification to ensure that data cannot be manipulated or changed without authorisation [8].

c. Cryptographic Strength:

The implementation of blockchain technology uses the power of cryptography to ensure information security. The cryptographic algorithms applied to blockchain technology protect data in transit and store it securely in encrypted blocks. This helps prevent unauthorised access to important data and protects its integrity and confidentiality [9].

d. Challenges and Drawbacks:

While the implementation of blockchain technology offers security benefits, the research also identified challenges and weaknesses associated with this technology. Examples include the level of scalability that needs to be improved, cost and performance that can be a bottleneck, and privacy-related concerns that arise in certain contexts [10].

The discussion of the results of this study shows the importance of being aware of and considering both advantages and disadvantages when considering the use of blockchain technology in improving information system security. The implementation of blockchain should consider the context of use, keeping in mind the specific needs, business objectives, and applicable regulations.

In conclusion, the implementation of blockchain technology can enhance information system security through decentralisation, transparency, and high cryptographic strength. However, the associated challenges and drawbacks must be well considered for the implementation to be successful. Further research and wider experiments need to be conducted to better understand the technical and practical aspects of implementing blockchain technology in improving

information system security.

5. CLOSURE

In this research, the implementation of blockchain technology in improving information system security has been studied and analysed. The results show that the application of blockchain technology can provide significant benefits in improving information system security. By using blockchain technology, data can be stored in a decentralised and securely encrypted manner. In addition, the consensus mechanism used in blockchain ensures that every transaction or data change must go through a strict verification process. This makes the information system more resistant to attacks and data manipulation.

Blockchain implementation can also improve data integrity by providing high auditability. Every transaction recorded on the blockchain cannot be altered or deleted unilaterally, allowing for a reliable audit trail. This will help in detecting and preventing unauthorised activities or misuse of data. In addition, blockchain technology can also increase the transparency of information systems. With an open and distributed mechanism, anyone can view and verify transactions that occur within the blockchain network. This will strengthen trust between users and information systems and reduce the potential for fraud.

In conclusion, the implementation of blockchain technology in information systems has great potential in improving security, integrity, and transparency. However, further research and development is needed to understand more deeply the challenges and potential in adopting this technology. It is hoped that this research can make a positive contribution to the development of more secure and reliable information systems in the future.

REFERENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

[2] Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

[3] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio.

[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). *Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services*, 14(4), 352-375.

[5] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends*. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.

[6] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). *A survey on the security of blockchain systems*. Future Generation Computer Systems, 81, 326-337.

[7] Yuan, Y., Ren, Y., Zhang, Z., Song, Y., & Lai, C. (2019). *Blockchain-based data security and privacy protection mechanisms for IoT data*. IEEE Internet of Things Journal, 6(5), 8244-8256.

[8] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., & Bass, L. (2017). *A taxonomy of blockchain-based systems for architecture design*. In 2017 IEEE International Conference on Software Architecture (ICSA) (pp. 243-252). IEEE.

[9] Zheng, Z., Xie, S., Dai, H., Wang, H., & Wang, L. (2016). *An empirical study on the security of key management schemes in blockchain systems*. In International Conference on Security and Privacy in Communication Systems (pp. 369-385). Springer.

[10] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). *Where is current research on blockchain technology?-A systematic review*. PloS one, 11(10), e0163477.