Indonesia Journal of Engineering and Education Technology (IJEET)
Volume 3 Nomor 1, hlm: 67-73
E-ISSN:3026-7544
Doi:10.61991/ijeet.v3i2.202

A Literature Review on the Role of Blockchain Technology in Enhancing Information System Security

Jusmawati[1], Tomi Apra Santosa[2]
[1] Universitas Yapis Papua, Indonesia
[2] AKademi Teknik Adikarya, Indonesia
Corresponding:juzmawati.nr@gmail.com

Abstract

This study aims to examine the role of blockchain technology in enhancing information system security. With increasing reliance on digital platforms, maintaining data integrity, confidentiality, and availability has become a major challenge. Blockchain, as a decentralized and immutable ledger system, offers a solution by providing transparency, audit trails, and resistance to manipulation. This study systematically analyzes recent research articles, case studies, and theoretical frameworks to evaluate how blockchain mechanisms such as cryptographic hashes, consensus protocols, and smart contracts contribute to strengthening information system security. The results demonstrate blockchain's potential in addressing vulnerabilities related to data leakage, fraud, and unauthorized access in various sectors, including finance, healthcare, and supply chain management. However, challenges such as scalability, regulatory compliance, and integration complexity are also critically discussed. This study aims to provide a comprehensive understanding of blockchain's capabilities and limitations in securing information systems and provide insights for future research and practical implementation.

Keywords: Blockchain, Information System Security, Decentralized Technology, Smart Contracts

Abstrak

Penelitian ini bertjuan membahas peran teknologi blockchain dalam meningkatkan keamanan sistem informasi. Dengan semakin besarnya ketergantungan pada platform digital, menjaga integritas, kerahasiaan, dan ketersediaan data menjadi tantangan utama. Blockchain, sebagai sistem buku besar terdesentralisasi dan tidak dapat diubah, menawarkan solusi dengan menyediakan transparansi, jejak audit, dan tahan terhadap manipulasi. Studi ini secara sistematis menganalisis artikel penelitian terkini, studi kasus, dan kerangka teori untuk mengevaluasi bagaimana mekanisme blockchain seperti hash kriptografi, protokol konsensus, dan smart contract berkontribusi dalam memperkuat keamanan sistem informasi. Hasil kajian menunjukkan potensi blockchain dalam mengatasi kerentanan yang berkaitan dengan kebocoran data, penipuan, dan akses tidak sah di berbagai sektor, termasuk keuangan, kesehatan, dan manajemen rantai pasok. Namun, tantangan seperti skalabilitas, kepatuhan regulasi, dan kompleksitas integrasi juga dibahas secara kritis. Kajian ini bertujuan memberikan pemahaman komprehensif mengenai kemampuan dan keterbatasan blockchain dalam mengamankan sistem informasi serta memberikan wawasan untuk penelitian dan implementasi praktis di masa depan.

Kata Kunci: *Blockchain*, Keamanan Sistem Informasi, Teknologi Desentralisasi, *Smart Contract*

Introduction

The rapid growth of digital services and the interconnected device ecosystem has increased the attack surface and the complexity of threats to information systems(Nawari & Ravindran, 2019). Incidents affecting service availability, such as DDoS attacks and ransomware, as well as exploiting vulnerabilities in edge devices and legacy components, continue to increase(Le & Hsu, n.d.), causing operational disruptions and significant financial and reputational losses (European Union Agency for Cybersecurity [ENISA], 2024). Furthermore, the volume and variety of reported vulnerabilities indicate that many systems remain vulnerable to automated exploits and software supply chain disruptions, necessitating a layered approach and proactive vulnerability management processes (ENISA, 2024; Taylor, 2020).

Data integrity and unauthorized access issues also pose crucial challenges: log manipulation, data changes without adequate audit trails, and weaknesses in authentication and authorization mechanisms open up opportunities for information leakage and misuse, which can have long-term impacts on stakeholder trust(Kademeteme & Bvuma, 2024). Furthermore, many traditional architectures still contain single points of failure (SPoFs), which leave entire services vulnerable when a single critical component is compromised, exacerbating the consequences of an attack or technical failure(Ghosh, 2019). Therefore, the literature emphasizes the need to integrate cryptographic techniques, distributed architectures, and tamper-resistant audit mechanisms to improve the resilience and reliability of information systems (Taylor, 2020; Punia et al., 2024).

Blockchain is a tamper-evident distributed digital ledger where transactions are recorded in cryptographically linked blocks, making them difficult to alter once published. It typically operates without a central authority (decentralization) (Yaga et al., 2018). Its key characteristics include decentralization (data replication across multiple nodes and a consensus mechanism), immutability (blockchains and hash functions that make record changes detectable), transparency (transaction records that can be audited by participants or authorized parties based on a permissioned model), the use of cryptography (hashes and digital signatures for authentication and integrity), and the ability to run smart contract programs that automatically execute business rules on the ledger. This combination of features distinguishes blockchain from traditional centralized storage and forms the technical basis for why this technology is often studied as a tool for improving information security assurance (Alanzi & Alkhatib, 2022); (Chattu et al., n.d.);(Liu et al., 2021).

Blockchain's relevance to information system security lies in its ability to fundamentally strengthen data integrity, availability, auditability, and non repudiation. Immutability and cryptography help ensure that data changes can be detected and that proof of origin and record integrity are maintained, making it suitable for audit logs and transaction records that are sensitive to manipulation(Sharma et al., 2020). Decentralization reduces the risk of single points of failure because data is replicated across multiple nodes increasing resilience to disruptions or attacks targeting a central entity; while smart contracts enable the automated enforcement of access and control policies consistent with defined security rules (e.g., role-based access, condition verification before execution). However, practical implementations need to consider limitations such as scalability, privacy (the need to obfuscate data on public ledgers or incorporate off-chain/zero-knowledge solutions), and governance and permission models meaning blockchain is a promising tool for improving certain aspects of information security, but not a single solution without compromise and careful design (Yaga et al., 2018).

Various systematic studies and literature reviews indicate that blockchain is often considered a solution to improve key aspects of information system security, particularly data integrity, auditability, and resilience to single points of failure(Nugroho et al., 2023); (Dong et al., 2023). An

early systematic study by Yli Huumo et al. (2016) positioned blockchain as a technology with broad potential but also with many unsolved research challenges; a further study by Casino, Dasaklis, and Patsakis (2019) classified blockchain applications across diverse domains including finance, supply chain, healthcare, Internet of Things (IoT), identity management, and recordkeeping and auditing showing that the empirical and conceptual literature is directing the attention of practitioners and researchers to the use of distributed ledgers for information security purposes such as data manipulation prevention, tamper-resistant auditing, and distributed access control mechanisms (Yli Huumo et al., 2016; Casino et al., 2019).

Based on this, this study aims to determine a Literature Review on the Role of Blockchain Technology in Enhancing Information System Security.

Research Methods

The research method used in this study uses a literature review approach to analyze the role of blockchain technology in enhancing information system security. The SLR process is structured through a series of steps, including problem identification, research question formulation, keyword selection, and inclusion and exclusion criteria. Literature sources were obtained from reputable scientific databases such as Scopus, IEEE Xplore, ScienceDirect, and Google Scholar, with publications spanning specific years to ensure the relevance and novelty of the research findings. Article selection was conducted through a multi-step screening process, including evaluation of titles, abstracts, and content, to ensure that only studies meeting methodological and academic relevance criteria were included.

Next, the selected articles were analyzed using thematic analysis techniques to identify patterns, key concepts, and findings related to blockchain's contribution to information system security. The analysis focused on aspects such as decentralization mechanisms, cryptography, data integrity, resilience to cyberattacks, and its implementation in various domains. Data from each study was coded and categorized to produce a comprehensive theoretical synthesis. The results of this analysis were then used to formulate conclusions describing the effectiveness, challenges, and potential of blockchain implementation in enhancing information system security. This systematic approach ensures that the literature review is objective, measurable, and replicable.

Result and Discussion

Blockchain Mechanisms that Contribute to Information System Security

Blockchain provides fundamental mechanisms that contribute significantly to improving information system security, one of which is through decentralization.(Pradeep et al., 2025) Unlike centralized systems that are vulnerable to single points of failure, blockchain architecture relies on a distributed peer-to-peer network, so that the failure of a single node does not affect the integrity of the entire system. This decentralization also reduces the risk of centralized attacks such as denial-of-service (DoS) and data manipulation by internal parties. By eliminating a single authority, blockchain creates an environment that is more resilient to systemic disruptions and exploits (Yli-Huumo et al., 2016). In addition to decentralization, cryptographic mechanisms are the foundation that strengthens blockchain security(Fetais, 2022). Each block and transaction is secured using cryptographic hashing algorithms such as SHA-256, which ensure that data cannot be altered without causing significant changes to the subsequent hash structure. Public-key cryptography mechanisms also enable strong entity authentication while maintaining transaction confidentiality through the use of public and private keys. Thus, cryptography in blockchain provides dual protection in the form of data integrity and authentication (Narayanan et al., 2016).

The next mechanism that plays a major role is consensus algorithms, procedures that ensure all nodes in the network reach agreement on the validity of transactions without the need for an

authoritative party. Algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) form a collective verification system that is difficult to manipulate, because changes to the ledger require control of a majority of computing power or capital. This consensus process protects the blockchain from attacks such as double-spending and prevents malicious entities from unilaterally altering data (Zheng et al., 2017). Immutability, or the inability to alter data once it has been recorded, is a crucial security contribution. Each block is linked through a cryptographic hash, so changes to one block affect the entire subsequent chain. This structure makes the blockchain highly resistant to data manipulation, especially in the context of auditing and transaction tracking(Ahmed, 2025). Immutability strengthens trust in information systems by ensuring that historical data cannot be altered without detection, a significant advantage over traditional databases (Crosby et al., 2016). Another mechanism that strengthens security is the use of smart contracts, which are automated programs that run on the blockchain and transparently execute rules. Because smart contracts are self-executing and stored in an immutable ledger, this mechanism reduces the risk of human error or fraud in transaction processing. Smart contracts also enable rule-based access control, thereby enhancing security controls in various digital business and government applications (Christidis & Devetsikiotis, 2016). Finally, blockchain supports security through auditability and transparency, as every transaction is recorded chronologically and can be traced by authorized parties. This mechanism increases accountability and enables rapid detection of suspicious activity. The combination of transparency, integrity, and traceability creates a very robust information security system, particularly in the context of supply chains, digital identity, and financial security. Thus, the overall blockchain mechanism forms a technological framework capable of enhancing the trustworthiness, resilience, and security of modern information systems (Bakhshi, 2018).

Security Enhancement Through Blockchain Implementation

Blockchain implementation has emerged as a strategic solution for enhancing information system security, primarily through the technology's ability to ensure high data integrity. Blockchain stores data in a structure of interconnected blocks using cryptographic hashes, ensuring that changes to one block cannot be made without altering the entire subsequent block. This mechanism makes stored data nearly impossible to manipulate(Saeed et al., 2022), reducing the risk of unauthorized data changes. Thus, organizations can leverage blockchain to maintain data authenticity in applications requiring high accuracy, such as financial systems, logistics, and medical records. Beyond data integrity, blockchain also enhances security by strengthening authentication and authorization processes. This technology enables the use of public-key cryptography to ensure that every entity in the network can be independently verified without the need for a central authority. The use of digital signatures ensures that transactions can only be executed by the authorized owner of the private key. Thus, blockchain provides a strong layer of protection against impersonation threats, identity theft, and unauthorized access to information systems (Gurtu & Johny, 2019); (Saeed et al., 2022);(Uluk et al., 2024).

Blockchain implementation also enhances network security through its decentralized nature. In a centralized system, an attack on a single critical point can lead to the failure of the entire system. However, blockchain distributes data and validation processes across all network nodes, so an attack on one or a few nodes doesn't affect the overall integrity of the network. This decentralization also increases resilience against Distributed Denial of Service (DDoS) attacks, as no single point can be a single target for system crippling. One very significant aspect of enhanced security through blockchain is the existence of smart contracts, which enable secure process automation. Smart contracts execute pre-programmed business rules autonomously without third-party intervention. Because these contracts are stored in an immutable ledger, the potential for system manipulation or abuse is significantly reduced. This feature is highly beneficial in applications such as supply chain

management, decentralized financial services (DeFi), and public administration, which require high transparency (Dong et al., 2023); (Singh, 2019).

Blockchain also strengthens security through enhanced auditability and transparency. Every transaction on the blockchain is permanently recorded and can be traced back to parties with designated access rights, creating an unfalsifiable audit trail. This transparency facilitates oversight, enables early detection of suspicious activity, and increases trust among stakeholders. In the context of cybersecurity, this capability supports the development of more accountable systems and minimizes the potential for fraud. Finally, the integration of blockchain with other technologies such as the Internet of Things (IoT) and artificial intelligence (AI) further expands its contribution to information system security. Blockchain can be used to secure communications between IoT devices through decentralized identities, reducing the risk of counterfeit device or man-in-the-middle attacks. Meanwhile, AI can leverage validated blockchain data to more accurately detect attack patterns. This combination creates a more adaptive, robust, and sustainable security ecosystem in the face of increasingly complex cyber threats (Alanzi & Alkhatib, 2022); (Delfi Kurnia Zebua et al., 2024; Hilmiyati et al., 2024; Zulyusri et al., 2023).

Challenges and Limitations of Blockchain in Information System Security

Although blockchain holds significant potential for enhancing information system security, the technology still faces significant challenges, particularly related to scalability. Consensus mechanisms such as Proof of Work (PoW) require significant computing capacity and slow transaction processing times. As the number of users and transaction volumes increase, public blockchain networks tend to become congested, reducing operational efficiency and effectiveness. This poses a major obstacle for organizations requiring fast, real-time data processing, such as financial services or large-scale digital transaction systems(Liu et al., 2021). Furthermore, blockchain faces limitations in interoperability, namely the ability of different blockchain platforms and traditional information systems to communicate with each other. The diversity of protocols, consensus mechanisms, and network architectures makes it difficult to build cohesive integration between systems. Without adequate interoperability, blockchain utilization at the organizational and interorganizational levels will be fragmented, hindering wide-scale adoption. This challenge demands the development of global standards and a more robust integration framework for blockchain to function optimally within the broader digital ecosystem (Han et al., 2023); (Alanzi & Alkhatib, 2022); (Asnur et al., 2024; Dewanto et al., 2023; Santosa et al., 2025).

Blockchain implementations also face vulnerabilities to certain attacks, despite their perceived high security. One example is a 51% attack, where an attacker who controls a majority of computing power can manipulate transactions on the network. Furthermore, smart contracts, a crucial component of blockchain applications, often have security vulnerabilities due to programming errors or poor design. These vulnerabilities can be exploited to steal digital assets or disrupt system logic. Therefore, while blockchain provides a robust security structure, certain technical aspects still require strict oversight and auditing (Saeed et al., 2022); (Han et al., 2023).

From a regulatory and governance perspective, blockchain faces significant challenges related to legal uncertainty and data privacy issues. Many jurisdictions lack a clear legal framework to regulate blockchain use, making organizations hesitant to fully adopt it. Furthermore, the transparent and immutable nature of blockchain raises privacy dilemmas, particularly in the context of data protection regulations such as the GDPR, which regulates the right to be forgotten. The tension between blockchain transparency and individual privacy protection is a major obstacle to implementing a compliant system(Kademeteme & Bvuma, 2024). Finally, blockchain adoption is also limited by the readiness of human resources and technological infrastructure. Blockchain implementation requires high-level technical expertise, both in architectural design, smart contract

development, and network security management. Many organizations still face competency gaps that hinder the effective implementation of this technology(Rijal & Saranani, 2023). Furthermore, the initial investment to build and maintain blockchain infrastructure is substantial, making it prohibitive for institutions with limited financial capacity. Overall, these challenges demonstrate that blockchain technology, while promising, still requires significant development and adaptation efforts before it can be optimally utilized in information systems security (Ahmed, 2025); (Sharma et al., 2020); (Rijal & Saranani, 2023).

Conclusion

The results demonstrate blockchain's potential in addressing vulnerabilities related to data leakage, fraud, and unauthorized access in various sectors, including finance, healthcare, and supply chain management. However, challenges such as scalability, regulatory compliance, and integration complexity are also critically discussed. This study aims to provide a comprehensive understanding of blockchain's capabilities and limitations in securing information systems and provide insights for future research and practical implementation.

References

Ahmed, S. (2025). *Enhancing Data Security and Transparency : The Role of Blockchain in Decentralized Systems*. *1*, 167–176.

Alanzi, H., & Alkhatib, M. (2022). *applied sciences Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology : A Systematic Review*.

Asnur, L., Jalinus, N., Faridah, A., Apra, T., Ambiyar, R. D., & Utami, F. (2024). *Video-blogs (Vlogs) -based Project : A Meta Analysis*. *14*(5), 1553–1557.

Chattu, V. K., Nanda, A., & Chattu, S. K. (n.d.). *The Emerging Role of Blockchain Technology Applications in Routine Disease Surveillance Systems to Strengthen Global Health Security*. 1–10.

Delfi Kurnia Zebua, Tomi Apra santosa, & Fegid Dian Putra. (2024). The Role of HR Analytics in Enhancing Organizational Performance: A Review Literature. *Indonesia Journal of Engineering and Education Technology (IJEET)*, *2*(2), 363–368. https://doi.org/10.61991/ijeet.v2i2.69

Dewanto, D., Wantu, H. M., Dwihapsari, Y., Santosa, T. A., & Agustina, I. (2023). Effectiveness of The Internet of Things (IoT)-Based Jigsaw Learning Model on Students' Creative Thinking Skills: A- Meta-Analysis. *Jurnal Penelitian Pendidikan IPA*, *9*(10), 912–920. https://doi.org/10.29303/jppipa.v9i10.4964

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). *Blockchain technology and application : an overview*. 1–50. https://doi.org/10.7717/peerj-cs.1705

Fetais, N. (2022). *Blockchain Technology for Intelligent Transportation Systems : A Systematic Literature Review*.

Ghosh, J. (2019). *The Blockchain : Opportunities for Research in Information Systems and Information Technology The Blockchain : Opportunities for Research in Information Systems*. *6846*. https://doi.org/10.1080/1097198X.2019.1679954

Gurtu, A., & Johny, J. (2019). *Potential of blockchain technology in supply chain management : a literature review*. *49*(9), 881–900. https://doi.org/10.1108/IJPDLM-11-2018-0371

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). *International Journal of Accounting Accounting and auditing with blockchain technology and artificial Intelligence : A literature review*. *48*(November 2022).

Hilmiyati, F., Panggabean, T. E., Khoirunnisa, R. N., Siregar, M. S., & Santosa, T. A. (2024). The Effectiveness of the CIPP Evaluation Model in Science Learning in the Era of the Industrial Revolution 4 . 0. *Jurnal Obsesi: Jurnal Pendidikan Anak Usia Dini*, *8*(6), 1375–1384. https://doi.org/10.31004/obsesi.v8i6.6227

Kademeteme, E., & Bvuma, S. (2024). *Using Blockchain Technology to Improve the Integrity and Transparency of Procurement Processes between SMMEs and Government : A Systematic Literature Review*. *7*(1), 1–12.

Le, T., & Hsu, C. (n.d.). *A Systematic Literature Review of Blockchain Technology : Security Properties , Applications and Challenges*. 789–802. https://doi.org/10.53106/160792642021072204007

Liu, M., Yeoh, W., Jiang, F., Choo, K. R., Liu, M., & Yeoh, W. (2021). *Blockchain for Cybersecurity : Systematic Literature Review and Classification Blockchain for Cybersecurity : Systematic Literature Review and Classification*. https://doi.org/10.1080/08874417.2021.1995914

Nawari, N. O., & Ravindran, S. (2019). *BLOCKCHAIN TECHNOLOGY AND BIM PROCESS : REVIEW AND POTENTIAL APPLICATIONS*. *24*(May), 209–238.

Nugroho, A., Putro, S., Mokodenseho, S., Hunawa, N. A., & Mokoginta, M. (2023). *Enhancing Security and Reliability of Information Systems through Blockchain Technology : A Case Study on Impacts and Potential*. *1*(01), 35–43.

Pradeep, A. S. E., Yiu, T. W., & Amor, R. (2025). *LEVERAGING BLOCKCHAIN TECHNOLOGY IN A BIM WORKFLOW : A LITERATURE REVIEW*. *2019*(November), 371–380.

Rijal, S., & Saranani, F. (2023). *The Role of Blockchain Technology in Increasing Economic Transparency and Public Trust*. *1*(2), 56–67. https://doi.org/10.61100/tacit.v1i2.51

Saeed, H., Id, H. M., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., Imran, M., & Khan, A. (2022). *Blockchain technology in healthcare : A systematic review* (Issue ii).

Santosa, T. A., Ali, M., Safar, M., Amri, M., Ruchiat, A., & Sjoraida, D. F. (2025). Inquiry-Based Learning and Critical Thinking Skills of Higher Education Students in the Era of Revolution 5 . 0 : A Meta-analysis. *CUESTIONES DE FISIOTERAPIA*, *54*(3), 5156–5166.

Sharma, P., Jindal, R., & Borah, M. D. (2020). *Blockchain Technology for Cloud Storage : A Systematic*. *53*(4).

Singh, P. (2019). *The Potentials and Impacts of Blockchain Technology in Construction Industry : A Literature Review The Potentials and Impacts of Blockchain Technology in Construction Industry : A Literature Review*. https://doi.org/10.1088/1757-899X/495/1/012005

Uluk, E., Masruchiyah, N., Nurhayati, R., Agustina, I., Sari, W. D., Santosa, T. A., Widya, U., Klaten, D., & Yogyakarta, U. N. (2024). Effectiveness of Blended Learning Model Assisted By Scholoogy to Improve Language Skills of Early Childhood Education Teachers. *Jurnal Obsesi: Jurnal Pendidikan Anak Usia Dini*, *8*(6), 1363–1374. https://doi.org/10.31004/obsesi.v8i6.6226

Zulyusri, Z., Santosa, T. A., Festiyed, F., Yerimadesi, Y., Yohandri, Y., Razak, A., & Sofianora, A. (2023). Effectiveness of STEM Learning Based on Design Thinking in Improving Critical Thinking Skills in Science Learning: A Meta-Analysis. *Jurnal Penelitian Pendidikan IPA*, *9*(6), 112–119. https://doi.org/10.29303/jppipa.v9i6.3709