Blockchain Technology for Enhancing Cryptocurrency Transaction Security in Indonesia: A Systematic Literature Review

Pourman Sitio[a1], Aldo Exaudi Sianipar[a2], Elonsius Manik[a3], Sartika Br Marbun[a4], Yohana Oktavia Haloho[a5], Santa Eliza Sitanggang[a6], Jeni Rifkayani Marpaung[a7],Sudarto[a8]
[a] Fakultas Informatika, Universitas Mikroskil, Indonesia
e-mail: : [1]221121287@students.mikroskil.ac.id, [2]221121070@students.mikroskil.ac.id,
[3]221121681@students.mikroskil.ac.id, [4]221122211@students.mikroskil.ac.id,
[5]221121772@students.mikroskil.ac.id, [6]221120604@students.mikroskil.ac.id,
[7]221121163@students.mikroskil.ac.id, [8]sudarto@mikroskil.ac.id

Abstrak

Penelitian ini mengkaji pentingnya teknologi Blockchain dalam memperkuat keamanan sistem Internet of Things (IoT), khususnya terkait mekanisme autentikasi dan integritas data. Dengan menggunakan pendekatan tinjauan literatur sistematis (SLR), penelitian ini melibatkan penyusunan pertanyaan penelitian, pencarian literatur yang komprehensif, penetapan kriteria inklusi dan eksklusi, pemilihan studi yang relevan, serta pengolahan dan analisis data untuk menarik kesimpulan. Hasil penelitian menunjukkan bahwa Blockchain secara signifikan meningkatkan keamanan IoT dengan menyediakan teknik autentikasi yang tangguh untuk memastikan hanya perangkat yang berwenang yang dapat mengakses jaringan, serta meningkatkan integritas data melalui catatan transaksi yang tidak dapat diubah. Temuan ini menyoroti potensi Blockchain dalam mengatasi kelemahan keamanan dalam kerangka kerja IoT. Secara ringkas, penelitian ini menekankan peran kritis Blockchain dalam mengamankan ekosistem IoT dan membangun kepercayaan di antara pengguna dan pemangku kepentingan. Penelitian masa depan sebaiknya fokus pada mengatasi masalah skalabilitas dan interoperabilitas untuk memaksimalkan efektivitas Blockchain dalam keamanan IoT.

Kata kunci: *Blockchain, Mata Uang Kripto, Keamanan Transaksi, Tinjauan Literatur Sistematis*

Abstract

This study explores the significance of Blockchain technology in bolstering the security of Internet of Things (IoT) systems, particularly concerning authentication and data integrity mechanisms. Utilizing a systematic literature review (SLR) approach, the research involves formulating research questions, performing extensive literature searches, setting inclusion and exclusion criteria, selecting pertinent studies, and processing and analyzing the data to draw conclusions. The findings indicate that Blockchain considerably enhances IoT security by offering robust authentication techniques that ensure only authorized devices gain network access, in addition to improving data integrity through unalterable transaction records. These results highlight Blockchain's potential to address security weaknesses within IoT frameworks. In summary, this research emphasizes the critical role of Blockchain in securing IoT ecosystems and building trust among users and stakeholders. Future investigations should aim to tackle scalability and interoperability issues to maximize the effectiveness of Blockchain in IoT security.

Keywords : *Blockchain, Cryptocurrency, Transaction Security, Systematic Literature Review*

1. Introduction

In the past decade, digital technology has significantly transformed financial systems worldwide, including in Indonesia, with cryptocurrencies being a key innovation. These digital

currencies enable fast cross-border transactions without the need for conventional financial intermediaries. The rise in crypto asset users in Indonesia, as shown by data from the Commodity Futures Trading Regulatory Agency (Bappebti), highlights the growing public trust in digital financial technologies and their potential as an alternative investment and transaction tool [1]. This shift is part of a broader social and economic transformation, driven by increased digital literacy, better access to mobile and internet technologies, and a growing interest in alternatives to traditional banking .

However, the rapid adoption of cryptocurrencies brings significant challenges, especially regarding transaction security. Cybercrimes such as hacking, phishing, fraud, and data manipulation are persistent risks in cryptocurrency transactions [2]. The lack of centralized oversight, coupled with the anonymity of crypto platforms, makes tracking and addressing abuses difficult. Moreover, the irreversible nature of most cryptocurrency transactions increases the risk, as fraudulent activities often result in irreversible financial losses . These security vulnerabilities underline the need for secure, transparent, and auditable systems that can provide trust and integrity in digital financial operations [3].

Blockchain technology offers a potential solution to these security issues. As a decentralized and distributed ledger, blockchain records transactions in a permanent, encrypted, and transparent manner [4]. The use of cryptographic mechanisms ensures that each block is securely connected, making data manipulation virtually impossible. Blockchain also supports automated verification through smart contracts, which execute predefined actions when specific conditions are met, reducing the need for human intervention and enhancing overall security . This decentralized model, backed by consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), ensures that no single actor controls the data, thus improving trust and reliability [5] .

While international studies have demonstrated the benefits of blockchain in securing digital transactions, there is limited research on its application in Indonesia [7]. Local studies have yet to address how blockchain can improve the security of crypto transactions within the Indonesian context, particularly in terms of digital infrastructure, regulatory frameworks, public literacy, and industry support . Additionally, cultural, social, and economic factors specific to Indonesia may affect the adoption and successful implementation of blockchain technology. Understanding these factors is crucial for developing solutions that are both technologically robust and socially acceptable [6].

This study employs a Systematic Literature Review (SLR) to examine blockchain-based crypto transaction security in Indonesia. The review focuses on relevant peer-reviewed publications from 2021 to 2025, ensuring that conclusions are evidence-based and applicable to local contexts. It also aims to identify key components for the successful implementation of blockchain in Indonesia, including cryptographic algorithms, consensus protocols, and the societal factors influencing user trust and digital literacy .

2. Research Method / Proposed Method

The Systematic Literature Review (SLR) method was used in this study to obtain a comprehensive, systematic, and objective review of how blockchain technology improves the security of cryptocurrency transactions in Indonesia. This study chose the SLR method because it provides a comprehensive understanding of previous research findings and reduces the possibility of bias arising during the analysis process. With SLR, this study can identify research gaps, analyze current findings, and provide an outline for further research.

2.1 Formulating research questions

The initial stage of this research began with formulating research questions to determine the direction of the study and the focus of the analysis. The main questions that formed the basis of this research included:
1. RQ1 : How does blockchain technology improve the security of crypto transactions?
2. RQ2 : What are the challenges of its implementation in Indonesia?

These questions are used to guide the process of searching and filtering literature to suit the research objectives.

2.2 Approaching literature searches

The literature search was conducted systematically through several credible academic databases, such as Scopus, Web of Science, IEEE Xplore, ScienceDirect, and Google Scholar. The keywords used in the search process were tailored to the research focus, namely Blockchain, Cryptocurrency, Transaction Security, and Indonesia. This combination of keywords was used to ensure that the literature found was relevant to the research topic. The search was conducted on publications published between 2021 and 2025 to ensure the relevance of the data to the latest technological developments.

2.3 Inclusion and exclusion criteria
Inclusion and exclusion criteria were determined to ensure that the literature analyzed was truly relevant and of high quality.

Table 1. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
indexed national or international journals	articles outside the specified time frame,
publications between 2021 and 2025	non-peer-reviewed articles such as blogs or white papers, and
discussing topics related to blockchain, crypto, and security, and	articles not relevant to the main focus of this research.
relevant to the Indonesian context, if available.	

2.4 Selecting and assessing article quality
A total of 25 scientific publications that met the initial criteria were found after conducting a literature search. After that, the articles were evaluated for quality and relevance to the research focus. To ensure the reliability and suitability of each publication used, a quality assessment (QA) method was used. The results of this process ensured that only articles with high credibility were used and that the blockchain technology used for further analysis made a significant contribution to the issue of cryptocurrency transaction security

2.5 Extracting data
The final stage in the SLR process is the extraction of data from each selected article. The types of data extracted include: (1) article identity (title, author, and year of publication), (2) key findings related to the role of blockchain in cryptocurrency transaction security, (3) proposed or implemented blockchain security mechanisms, (4) implementation challenges in the Indonesian context, and (5) experimental or simulation results that support the effectiveness of this technology. All data obtained from the extraction process is then analyzed descriptively and compared to produce a comprehensive synthesis of blockchain's contribution to cryptocurrency transaction security in Indonesia.Contains an explanation of the stages of research that illustrates the logical sequence to get research output in line with expectations.

3. Literature Study
The literature study conducted for this research focuses on blockchain technology and its application to improve the security of cryptocurrency transactions, particularly within Indonesia. A systematic literature search was conducted across various academic databases such as Scopus, Web of Science, IEEE Xplore, ScienceDirect, and Google Scholar, using keywords such as Blockchain, Cryptocurrency, Transaction Security, and Indonesia. The selected publications were limited to peer-reviewed articles published between 2021 and 2025 to ensure that the data reflects the latest technological developments.

The inclusion criteria for the literature review were articles that specifically discussed blockchain technology, its role in securing cryptocurrency transactions, and the implementation of blockchain in the Indonesian context. Articles that were published outside the specified time frame, non-peer-reviewed articles such as blogs or white papers, and those not relevant to the research focus were excluded from the review.

After conducting the literature search, a total of 25 scientific articles were identified. These articles were evaluated based on their relevance, methodological rigor, and data reliability. Seven articles were selected as the most relevant, as they provided valuable insights into the application of blockchain technology in enhancing the security of cryptocurrency transactions in Indonesia.

The selected articles were analyzed thematically, and key findings were synthesized. The studies highlighted that blockchain's decentralized nature, cryptographic encryption, and immutability provide robust security for digital transactions. However, challenges such as regulatory uncertainties, infrastructure limitations, and low digital literacy were also identified as significant barriers to blockchain adoption in Indonesia. These challenges need to be addressed for the successful implementation of blockchain technology in the Indonesian digital finance ecosystem.

4. Result and Discussion
4.1 Results

The results of the Systematic Literature Review (SLR), conducted in accordance with the steps outlined in the methods section, were 25 scientific publications that met all inclusion criteria and passed the quality test. During the period 2021–2025, these articles were obtained through a comprehensive search of various academic databases, including Google Scholar, Scopus, Web of Science, IEEE Xplore, and ScienceDirect.

The results of the identification process yielded 132 initial articles. Only 25 articles met the final criteria after passing the title and abstract screening stages and the application of inclusion-exclusion criteria. Of these 25 articles, 7 were selected as the most relevant to the research subject because they had a strong fit with the research topic, strong methodology, and made a significant contribution to the security aspects of blockchain-based crypto transactions in Indonesia. The following presents the results of quality assessment and data extraction for the 7 most relevant articles.

Table 2. Quality Assessment Results (Quality Assessment)

Code	Author(s) (Year)	Relevance (1–5)	Clarity of Methodology (1–5)	Data Reliability (1–5)	Total Score	Decision
A1	Kusuma et al. (2022)	5	5	5	15	Accepted
A2	Suraya et al. (2022)	4	5	5	14	Accepted
A3	Fahlevi et al. (2022)	5	4	4	13	Accepted
A4	Saputra & Darma (2022)	4	4	5	13	Accepted
A5	Fathiyana et al. (2022)	5	5	4	14	Accepted
A6	Suryawijaya & Wibowo (2023)	4	4	4	12	Accepted
A7	Sifaudin et al. (2024)	5	5	5	15	Accepted

The results of the quality assessment of the seven most relevant articles show that all publications meet methodological standards and data credibility, and are therefore deemed suitable for further analysis. Articles with codes A1 and A7 received the highest score of 15, indicating a very high level of relevance, methodological clarity, and data reliability. Several other articles, such as A2 and A5, also showed high quality with a total score of 14, mainly due to the clarity of the methodology and adequate empirical data support. Meanwhile, articles A3, A4, and A6 received slightly lower scores, ranging from 12 to 13, but were still considered to meet the minimum quality standards as they still made a significant contribution to the research focus. In general, these results prove that the selected literature has good academic consistency and is relevant to the research objectives on the application of blockchain technology in improving the security of cryptocurrency transactions in Indonesia.

The results of the thematic analysis conducted on seven selected studies investigating the use of blockchain technology in the context of cryptocurrency transaction security in Indonesia are presented in the following section. Each article was evaluated based on the main principles used, key findings supporting crypto security elements, and issues found in applications in Indonesia. The purpose of this table is to provide a comparative overview of the focus and contribution of each study. This is done to clarify the research path and areas that need further study.

Table 3. Summary of Thematic Findings

Code	Author	Main Mechanism	Core Findings on Crypto Security	Key Challenges in Indonesia
A1	Kusuma et al. (2022)[11]	Data Validity, Immutability, Smart Contract	Ensures data and process transparency; prevents falsification and corruption through decentralization.	Centralized systems are vulnerable to hacking; conventional processes trigger corruption.
A2	Suraya et al. (2022)[12]	Monetary Transparency, Auditability, Decentralization	Reduces embezzlement and ensures accountability through auditable and transparent monetary data.	Limited physical infrastructure, high implementation costs, and low financial literacy.
A3	Fahlevi et al. (2022)[13]	Security, Anti-Fraud	Security is identified as the most significant adoption factor; effectively reduces fraud, revenue manipulation, and agency conflict.	Regulatory frameworks remain non-adaptive; persistent agency conflict and fraud issues.
A4	Saputra & Darma (2022)[14]	Security, Trust	User trust strongly influences the intention to adopt blockchain-based financial applications.	Unclear or inconsistent crypto regulations; technical reliability issues (bugs, delays).
A5	Fathiyana et al. (2022)[15]	Decentralization, Data Integrity, Immutability	Eliminates single points of failure and prevents data misuse; guarantees high data integrity.	Centralized systems remain vulnerable to hacking and unauthorized data manipulation.
A6	Suryawijaya & Wibowo (2023)[16]	Decentralization, Encryption, Integrity	Provides stronger data protection through encryption and decentralization; high integrity by preventing data modification; reduces fraud risk.	Unclear or inconsistent regulations; limited internet infrastructure; scalability constraints.
A7	Sifaudin et al. (2024)[17]	Institutional and Technological Trust	Institutional and technological trust significantly influence Gen Z's intention to adopt; institutions play a key role in ensuring security.	Low adoption readiness due to inadequate infrastructure and persistent privacy/security concerns.

The results of the thematic analysis conducted on seven selected studies investigating the use of blockchain technology in the context of cryptocurrency transaction security in Indonesia are presented in the following section. Each article was evaluated based on the main principles used, key findings supporting crypto security elements, and issues found in applications in Indonesia. The purpose of this table is to provide a comparative overview of the

focus and contribution of each study. This is done to clarify the research path and areas that need further study.

4.2 Discussion

1. RQ1 : Improved Security for Crypto Transactions

The enhancement of cryptocurrency transaction security through blockchain technology does not stem from a single element, but rather from the integration of multiple core mechanisms such as decentralization, encryption, immutability, and transparency through a shared ledger. Based on findings from the seven selected studies, blockchain's advantage lies in its ability to combine cryptographic systems with network consensus mechanisms to maintain the integrity and validity of transaction data. By utilizing a distributed approach, blockchain effectively reduces reliance on a single authority and strengthens overall digital security layers.

Kusuma et al. (2022) highlight that data validity and the implementation of smart contracts form a crucial foundation for preventing forgery and bribery in digital transaction systems. Smart contracts enable agreements to be executed automatically without third-party intervention, minimizing opportunities for data manipulation or contract breaches. Furthermore, the immutability feature of blockchain ensures that recorded transactions cannot be altered or deleted, creating a permanent and transparent audit trail [11].

Suraya et al. (2022) emphasize the importance of monetary transparency and auditability in establishing an accountable transaction system. Blockchain allows all network participants to verify transaction records openly, reducing the risk of embezzlement and accounting errors[12]. This transparency not only increases user trust but also strengthens financial oversight mechanisms. However, Suraya also notes implementation challenges in Indonesia, such as high infrastructure costs and low financial literacy, which could hinder optimal adoption. Meanwhile, Fahlevi et al. (2022) find that security is the most influential factor in driving blockchain adoption, particularly among investors and financial institutions. Their research demonstrates that blockchain's decentralized system significantly reduces fraud, revenue manipulation, and agency conflicts often seen in traditional financial systems. Through transaction validation based on consensus, all economic activities are verified by the entire network rather than a single controlling entity[13].

Saputra and Darma (2022) add that users' trust perception significantly affects their intention to adopt blockchain. When users are confident in system integrity and minimal risk of data leakage, adoption rates increase substantially. This trust is built through transparency, auditability, and a reliable system that operates without control from a single authority. Nevertheless, they highlight that cryptocurrency regulations in Indonesia remain reactive and not fully adaptive to emerging digital technologies[14].

Fathiyana et al. (2022) deepen the discussion on decentralization and data integrity by stressing that blockchain eliminates single points of failure, where a failure in one node could jeopardize the entire system. In conventional systems, such as electronic certificates or centralized corporate governance, attacks on the main server could have catastrophic effects. Blockchain, by distributing data across multiple nodes, ensures that failure at a single point does not compromise the overall system, making it more resilient against hacking and data misuse[15].

The contribution of Suryawijaya & Wibowo (2023) underscores the importance of combining strong encryption with decentralization to maintain data integrity and confidentiality[16]. Each transaction block is secured using complex cryptographic algorithms, making data alteration nearly impossible without majority node approval. Their findings also highlight that high integrity is critical in reducing fraud risk, especially in digital financial transactions. Nonetheless, they caution that regulatory uncertainty from Bank Indonesia (BI) and the Financial Services Authority (OJK) remains a barrier to nationwide adoption.

Sifaudin et al. (2024) introduce a social and psychological dimension, focusing on institutional and technological trust[17]. Digitally native generations, such as Gen Z, are more likely to adopt blockchain if there is assurance of security from official institutions and the system is perceived as reliable. They emphasize that trust in regulatory authorities plays a crucial role in mitigating perceived risks regarding privacy and access security. However, they note that improving digital literacy alone is insufficient without robust infrastructure and regulatory support.

Overall, these seven studies demonstrate that advanced cryptographic encryption, distributed consensus, and an immutable ledger are complementary components in ensuring cryptocurrency transaction security. Together, they create a transparent, secure, and tamper-resistant ecosystem. This synergy gives blockchain an advantage over centralized systems, which are more susceptible to misuse by single authorities. However, successful implementation in Indonesia depends on digital infrastructure readiness, clear legal frameworks, and increased public trust in regulatory institutions. In conclusion, the enhancement of cryptocurrency transaction security through blockchain represents not just a technological innovation, but a paradigm shift in digital governance. Blockchain introduces a new model of trust based on algorithms and mathematical proof, rather than institutional authority. Although implementation challenges remain, the findings indicate that blockchain has significant potential to serve as a strategic solution for strengthening digital transaction security in Indonesia, while also laying the foundation for a more transparent, efficient, and reliable financial ecosystem.

2. RQ2: Challenges of Blockchain Implementation in Indonesia

The adoption of blockchain technology in Indonesia faces a range of challenges that extend beyond technical implementation, encompassing regulatory, infrastructural, and social dimensions. Insights from the seven selected studies indicate that while blockchain offers robust security and transparency for cryptocurrency transactions, several contextual factors affect its practical deployment in the Indonesian ecosystem. One major challenge highlighted by Suraya et al. (2022) is the limited financial literacy and awareness among the general population[12]. Despite blockchain's ability to provide auditable and tamper-proof transaction records, many potential users struggle to understand the technology and its benefits. This lack of understanding can slow adoption rates and reduce confidence in digital financial systems, particularly among small investors or communities with limited exposure to digital finance.

Regulatory uncertainty is another prominent obstacle. Saputra & Darma (2022) and Suryawijaya & Wibowo (2023) emphasize that the absence of clear and adaptive regulations regarding cryptocurrency and blockchain applications has created ambiguity for both users and institutional stakeholders[14], [16]. In some cases, Bank Indonesia (BI) and the Financial Services Authority (OJK) maintain a cautious stance, which can discourage startups and businesses from fully implementing blockchain solutions. Without a clear legal framework, users may perceive higher risks, particularly related to fraud, privacy, and legal recourse.

Infrastructure limitations also pose significant constraints. Studies by Suraya et al. (2022) and Fathiyana et al. (2022) highlight that inconsistent internet connectivity, limited network bandwidth in remote areas, and high operational costs for deploying blockchain nodes can impede scalability. Decentralized networks require reliable connectivity across nodes to maintain data integrity, and infrastructure gaps can slow transaction processing or reduce system reliability[12], [15].

Social and institutional trust is equally critical. Sifaudin et al. (2024) find that Gen Z and other digitally savvy users are more likely to adopt blockchain when they trust both the technological system and the institutions overseeing it[17]. However, when institutional oversight is perceived as weak or inconsistent, users remain cautious. This underscores the need for trusted governance models and transparent regulatory enforcement to complement the technical strengths of blockchain.

Another challenge relates to the integration of blockchain with existing financial and organizational systems. Fahlevi et al. (2022) note that legacy systems in banks, government institutions, or enterprises may not be fully compatible with blockchain infrastructure[13]. The transition requires significant investments in technology, training, and organizational restructuring, which can slow adoption despite the demonstrated security advantages.

Finally, scalability and performance concerns remain a technical challenge. Suryawijaya & Wibowo (2023) highlight that high transaction volumes and network latency can limit blockchain's effectiveness in real-time financial operations[16]. While blockchain ensures security and transparency, ensuring speed and efficiency for large-scale commercial use is still a work in progress in Indonesia. In summary, while blockchain presents a promising framework for secure, transparent, and tamper-resistant cryptocurrency transactions, Indonesia's adoption is shaped by a combination of financial literacy, regulatory clarity, infrastructure readiness, institutional trust, and technical scalability. Addressing these multifaceted challenges requires coordinated efforts from regulators, financial institutions, technology providers, and educational

initiatives to foster public understanding and trust. Only through a holistic approach can blockchain technology realize its full potential within Indonesia's evolving digital economy.

5. Conclusion

Based on an analysis of 25 scientific journals, particularly the seven most relevant ones, it can be concluded that blockchain technology improves the security of crypto transactions in Indonesia because it ensures data integrity, validity, and transparency through decentralization mechanisms, complex encryption, smart contracts, and immutable storage. This system increases user trust and transaction auditability while reducing the risk of counterfeiting, manipulation, and fraud. Conversely, limited infrastructure, low digital and financial literacy, and unclear cryptocurrency regulations are some of the obstacles that still hinder the use of blockchain in Indonesia. As a result, blockchain adoption not only provides a technological solution to improve transaction security, but also requires technical readiness, regulatory support, and increased public awareness.

References

For Journal:
[1] O. Handayani, E. Masri, P. Rahayu, A. J. Pamungkas, and M. Azam, "Legal Framework For Crypto Asset Trading As An Effort To Protect Consumers In Indonesia," *Pena Justisia Media Komun. Dan Kaji. Huk.*, vol. 24, no. 2, pp. 8252–8273, Oct. 2025, doi: 10.31941/pj.v24i2.7134.
[2] M. S. K. Munira, "DIGITAL TRANSFORMATION IN BANKING: A SYSTEMATIC REVIEW OF TRENDS, TECHNOLOGIES, AND CHALLENGES," Jan. 27, 2025, *Social Science Research Network, Rochester, NY*: 5161354. doi: 10.2139/ssrn.5161354.
[3] "Cryptocurrency Scams: Analysis and Perspectives | IEEE Journals & Magazine | IEEE Xplore." Accessed: Nov. 03, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9591634
[4] U. Agarwal, V. Rishiwal, S. Tanwar, and M. Yadav, "Blockchain and crypto forensics: Investigating crypto frauds," *Int. J. Netw. Manag.*, vol. 34, no. 2, p. e2255, 2024, doi: 10.1002/nem.2255.
[5] "Blockchain as supply chain technology: considering transparency and security | International Journal of Physical Distribution & Logistics Management | Emerald Publishing." Accessed: Nov. 03, 2025. [Online]. Available: https://www.emerald.com/ijpdlm/article-abstract/51/3/305/162184/Blockchain-as-supply-chain-technology-considering?redirectedFrom=fulltext
[6] "The transparency challenge of blockchain in organizations | Electronic Markets." Accessed: Nov. 03, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s12525-022-00536-0
[7] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Netw.*, vol. 2021, no. 1, p. 6693731, 2021, doi: 10.1155/2021/6693731.
[8] M. Jin, X. Zhang, X. Yue, Q. Zuo, and J. Nie, "Consensus mechanism selection in Web 3.0 blockchain platforms: Proof of Work vs. Proof of Stake," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 200, p. 104173, Aug. 2025, doi: 10.1016/j.tre.2025.104173.
[9] I. G. M. T. Pradana, T. Djatna, I. Hermadi, and I. Yuliasih, "Readiness Assessment Framework and Integrated Participatory Development Approach for Blockchain-Based Traceability Systems: Case Study in Kintamani Coffee Agroindustry Supply Chain," *J. Soc. Comput.*, vol. 5, no. 4, pp. 344–362, Dec. 2024, doi: 10.23919/JSC.2024.0027.
[10] R. Z. Fathiyana, S. N. Yutia, and D. J. Hidayat, "Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology," *JOIV Int. J. Inform. Vis.*, vol. 6, no. 1, pp. 109–116, Mar. 2022, doi: 10.30630/joiv.6.1.877.
[11] T. W. E. Suryawijaya and M. E. S. Wibowo, "ENHANCING DATA SECURITY BY BLOCKCHAIN TECHNOLOGY: INVESTIGATING THE EFFECTIVE EXECUTION OF DIGITAL TRANSFORMATION INITIATIVES IN INDONESIA," *Glob. Policy J. Int. Relat.*, vol. 11, no. 02, Dec. 2023, doi: 10.33005/jgp.v11i02.4138.

[12] M. Sifaudin and N. Ayiyah, "The Future of Digital Finance: The Impact of Cryptocurrency and Blockchain on Digital Securities in Indonesia and Gen Z's Adoption Potential," *J. Bus. Manag. Islam. Bank.*, pp. 71–100, Dec. 2024, doi: 10.14421/jbmib.v3i1.2345

Proceeding:
[1] M. A. Kusuma, P. Sukarno, and A. A. Wardana, "Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia," in *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)*, Nov. 2022, pp. 1–6. doi: 10.1109/ICACNIS57039.2022.10055114
[2] M. Fahlevi, M. Moeljadi, S. Aisjah, and A. Djazuli, "Blockchain Security and Corporate Governance," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*, Oct. 2022, pp. 1–5. doi: 10.1109/ICORIS56080.2022.10031537.

Edited book:
[1] "The Intention to Use Blockchain in Indonesia Using Extended Approach Technology Acceptance Model (TAM)." Accessed: Nov. 03, 2025. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/89964860/4417-libre.pdf?1660979999=&response-content-disposition=inline%3B+filename%3DThe_Intention_to_Use_Blockchain_in_Indon.pdf&Expires=1762180755&Signature=DA55F9o4F~Qs~sup53BfGouaBZFS4Mg53nTElbLUg8mZeC5y1KwOpYZlArAsriO9nV-CfNajQXKDq8P3rua9edZH4QkO6JXqai7UpUPt7xWCv5VCrTpBg6UIeWULaVM3aAblq7asD2C1CLXLoRvWgvaJYJ3kYwB8kESoQInqGrWMlQIQXhI6Cq~rCri~DKax3il61Z7nv2yKisJh9gxu1fB455MjvoPwvoXcFbbgS3U6cqdTwNoncFfCr1LxFnVEpxqjEaHSoJNShkBTIIO2szsUgcUHBQwVl5yJA0rczVb0paF25dJ~hbYdUzaReA0gVpIijo-Zyt63Ys8pTrbMhA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.