TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 6, December 2026, pp. 1942~1950
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i6.27746

Blockchain implementation for digital transaction security: a systematic literature review

Ni Komang Dewi Mahayani, Yadhurani Dewi Amritha
Department of Information Technology, Faculty of Engineering and Informatics, Universitas Pendidikan Nasional, Bali, Indonesia

Article Info

Article history:

Received Dec 19, 2025
Revised Jul 19, 2026
Accepted Sep 8, 2026

Keywords:

Blockchain
Cybersecurity
Digital transaction security
Distributed ledger
Systematic literature review

ABSTRACT

Digital transactions are increasingly vulnerable to security threats, such as data manipulation, identity theft, fraud and cyber-attacks, making more reliable security mechanisms essential. This research systematically reviews the implementation of blockchain in digital transaction security, focusing on security mechanisms, potential threats, and its advantages and limitations. A systematic literature review (SLR) was performed on 100 scientific articles published between 2021 and 2025 through a process of identifying, selecting, evaluating, and inclusion based on pre-defined criteria. The research results show that blockchain enhances the integrity, transparency and security of transactions through an immutable distributed ledger, public-key cryptography, consensus mechanisms and smart contracts. These mechanisms can reduce data manipulation, fraud, identity-related threats and single points of failure, whilst also supporting transaction efficiency. However, scalability, latency, energy consumption, privacy and integration with legacy systems remain challenges. This research identifies a hybrid system that integrates conventional databases and blockchain technologies as a practically acceptable approach to balancing the security and efficient digital transactions.

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

Corresponding Author:

Ni Komang Dewi Mahayani
Department of Information Technology, Faculty of Engineering and Informatics
Universitas Pendidikan Nasional
Bali, Indonesia
Email: dewimahayani94@gmail.com

1. INTRODUCTION

Over the past decade, digital transformation has shifted the paradigm of financial transactions from traditional methods to an integrated digital ecosystem [1]. This digitalisation is not merely a trend, but a vital element of the modern economy, offering operational efficiency, reduced transaction costs and a massive expansion of financial inclusion across all sections of society [2]. However, the rapid digitisation of transactions has given rise to cyber threats such as phishing, malware and sophisticated data breaches, which continue to evolve beyond the capabilities of conventional system protections [3]. The implementation of blockchain could provide an alternative solution to these problems.

Various previous studies have shown that blockchain, as a new architecture, offers advanced security through decentralisation and cryptography [4]. Unlike concentrated systems, which are exposed to single points of failure, blockchain spreads data around a global network in the form of permanently signed (immutable) blocks [5]. This characteristic theoretically ensures transparency whilst automating administrative processes, making them faster and more efficient [6]. Nevertheless, the implementation of blockchain in digital transactions still has several issues to overcome, such as the scalability, privacy and

regulatory challenges. These challenges can affect performance, data protection, system integration and compliance with regulations in blockchain implementation.

Current literature reviews often focus solely on blockchain technology generally, but very few critically analyze the implementation of blockchain in digital transactions. This research addresses this gap by reviewing 100 articles related to the implementation of blockchain in digitized transactions, focusing on blockchain strategies and mechanisms for enhancing the protection of digital transactions, the types of security threats that are reduced through the use of blockchain, and the benefits and challenges of its implementation in digital transactions. Furthermore, this research presents a comparative analysis between blockchain security mechanisms and the National Institute of Standards and Technology (NIST) framework to evaluate blockchain's ability to support digital transaction security. In theory, this contribution adds to the study of decentralised cybersecurity. In practical terms, it is expected that the findings of this research will provide guidance for financial service providers in building a transaction infrastructure that is not only fast, but also able to withstand future threats.

2. METHOD

This review employs a systematic literature review (SLR) to evaluate the implementation mechanisms, security advantages and limitations of blockchain technologies in digitized transactions. The SLR consists of four (4) phases, which are: (i) formulation of the research question, (ii) selecting studies, (iii) extracting data, and (iv) synthesizing data [7]. The stages of this SLR begin by formulating the research questions, namely: (i) how does the implementation of blockchain ensure digital transaction security? (ii) what security threats are addressed by blockchain? and (iii) what are the advantages and limitations of implementing blockchain in digital transactions? the literature research was carried out using Scopus, Google Scholar and Sinta, as these databases provide reputable publications relevant to the topic. To increase search result accuracy, the literature search was carried out using a combination of keywords Boolean operator strategy as follows: ("blockchain" OR "distributed ledger technology") AND ("digital transaction security" OR "e-payment security" OR "fraud prevention").

The selection process of the research was following the preferred reporting items for systematic reviews and meta-analyses (PRISMA) standard, which comprises the stages of identification, screening, eligibility, and inclusion. The identification process yielded 420 articles; 390 of these were then selected and screened to obtain the full-text versions. From these, 150 articles underwent an eligibility assessment, resulting in 100 articles that fulfilled the inclusion criteria for the purposes of the analysis. The article selection process is outlined in Figure 1.

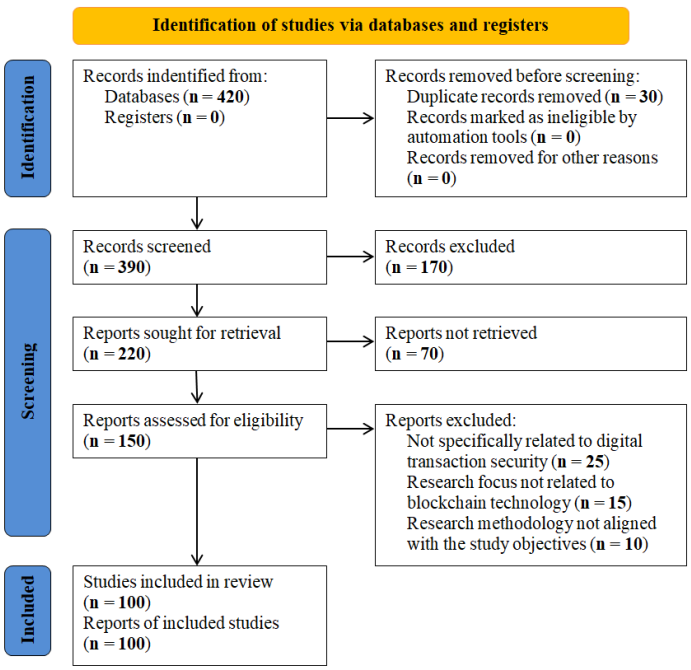


Figure 1. PRISMA flow diagram

Criteria for selecting these articles were established to make sure that these studies related directly to the objective of the research. The inclusion and exclusion guidelines for the selected articles were outlined in Table 1. Each article that met the inclusion criteria was analysed using thematic coding, which encompassed open coding, axial coding and selective coding, to identify, group and define the main themes of the research [8]. The coding process was carried out manually using Microsoft Excel. Quality assessment was carried out based on the objectives, methodology, relevance to digital transaction security, research findings, and the articles' contribution to blockchain development. Only articles of sufficient quality are eligible for inclusion in this review. During the synthesis stage, the articles were analysed qualitatively by grouping them thematically based on the mechanisms for implementing blockchain, security threats that can be addressed, and the advantages and limitations of its implementation. The purpose of this study is to identify trends in research and any remaining gaps, and to provide recommendations for future research.

Table 1. Inclusion and exclusion criteria for article selection

Inclusion criteria	Exclusion criteria
Studies on blockchain implementation for digital transaction security	Studies unrelated to digital transaction security
Peer-reviewed journal or conference paper (2021-2025) with a clear methodology and findings	Published outside 2021–2025, non-peer-reviewed, or lacking a clear methodology and findings
Full text available	Full text unavailable

A total of 100 studies, which have been screened and analysed, are considered representative as they cover a wide range of blockchain application areas, employ various research methods, and have been published in a variety of leading academic journals. This number is deemed sufficient to present a complete overview of research trends and technological developments in blockchain within the context of digital transaction security.

3. RESULTS AND DISCUSSION

3.1. Result

This SLR analysed 100 scientific journal articles to examine the implementation of blockchain in secure digital transactions. This research identified the mechanisms for implementing blockchain, Security threats that can be mitigated, and the advantages and limitations of its implementation. Results of this research has been outlined in Table 2.

Table 2. Thematic clusters based on research questions

No	Thematic cluster	Main topics of discussion	Article source
1	The implementation of blockchain in ensuring the security of digital transactions	Architecture design, protocols, consensus, smart contracts, identity, artificial intelligence (AI)/ internet of things (IoT) /cloud integration for transaction security	[9]-[61]
2	Security threats addressed through blockchain technology	Types of threats to digitized transactions and how blockchain can minimize these threats	[1], [3], [5], [62]-[85]
3	Advantages and limitations of blockchain implementation in digitized transactions	Efficiency, sustainability, trust, performance improvement, financial inclusion, as well as scalability, regulation, costs, blockchain risks, latency, technical complexity and governance	[6], [77], [86]-[103]

3.1.1. RQ1: how does the implementation of blockchain ensure the security of digital transactions?

Blockchain functions as a decentralised digital ledger that secures and verifies transactions through cryptography, consensus mechanisms and smart contracts. The combination of these mechanisms ensures authentication, integrity, confidentiality, immutability and transparency. Transaction security is underpinned by public-key cryptography and hash functions to safeguard data integrity. Smart contracts automatically verify transactions with no requirement from third parties, thereby minimising the threat of manipulated data. Various architectural and cryptographic strategies form the basis of blockchain security through the on-chain storage of transaction hashes, whilst large volumes of data are stored off-chain and secured using encryption such as advanced encryption standard (AES). Furthermore, technologies such as homomorphic encryption,

zero-knowledge proofs and multi-signatures enhance the protection of sensitive data. Consensus algorithms like proof-of-work (PoW), proof-of-stake (PoS) and practical byzantine fault tolerance (PBFT) validate transactions and avoid data manipulation. All transactions are logged as a transparent and immutable audit track, thereby supporting audit processes and security analysis.

3.1.2. RQ2: what security threats are addressed by blockchain?

Blockchain enhances the integrity and accessibility of data through an immutable distributed ledger. These characteristics make it difficult to manipulate data, falsify financial statements or misuse documents within digital transaction systems. Furthermore, blockchain helps to reduce financial crimes of various kinds, like money laundering, credit fraud and double-selling. When integrated with AI and ensemble models, blockchain can support the early detection of suspicious activity. Blockchain supports multi-factor and decentralized authentication in digital wallets, thereby reducing the threat of brute-force attacks, phishing, account takeovers and credential leaks. To enhance privacy, blockchain integrates technology like homomorphic encryption, zero-knowledge proofs and trace obfuscation to secure private data from identity disclosure. Furthermore, mechanisms such as cross-chain reputation management strengthen the network's resilience against specific security threats.

3.1.3. RQ3: What are the advantages and limitations of implementing blockchain in digital transactions?

The use of blockchain strengthens transaction integrity, transparency, and accountability by employing a tamper-resistant distributed ledger. This decentralized structure helps minimize data alteration and fraudulent activities while addressing security weaknesses associated with centralized systems. The decentralization and consensus systems of blockchain also eliminate the need for intermediaries in peer-to-peer transactions, thereby decreasing transaction costs and improving efficiencies. In addition, the integrated use of smart contracts, encryption, AI and digital identity approaches such as self-sovereign identity (SSI) supports automation, enhances threat and fraud detection, and strengthens security and trust within the digital transaction ecosystem.

Although it offers a range of advantages, the implementation of blockchain still faces a number of limitations. Public blockchains based on PoW suffer from scalability issues, slow transaction speeds and heavy energy usage, rendering them unsuitable for real-time applications without the support of solutions such as sidechains or off-chain storage. Furthermore, blockchain implementation requires significant investment costs, substantial computing resources, and specialist expertise to develop and manage both the network and smart contracts. The transparent nature of blockchain also has the potential to pose privacy risks if not supported by adequate data protection mechanisms. On the other hand, blockchain is not entirely immune to security threats, such as application vulnerabilities, social engineering, and weaknesses in network design or the economic model employed.

3.2. Discussion

A review of 100 articles shows that the application of blockchain in digital transaction security which integrates distributed ledgers, cryptography, decentralised architecture, consensus mechanisms and smart contracts can support integrity, authentication, confidentiality and non-repudiation. Its implementation is tailored to the system's requirements, including the use of a hybrid architecture where core data is stored off-chain whilst hashes and metadata are stored on-chain to maintain integrity. These findings indicate a trend towards more efficient blockchain implementation without compromising security.

The approach to blockchain security differs from that advocated by NIST. NIST emphasises security governance through identification, protection, detection, response and recovery. In contrast, blockchain enhances security through decentralisation, consensus, cryptography, distributed ledgers and smart contracts. The two can complement each other. NIST serves as a framework for governance and risk management, whilst blockchain serves as a technical security layer. An analysis mapping blockchain features to NIST functions is displayed in Table 3.

In terms of security mechanisms, cryptography, hashing, digital signatures, consensus and smart contracts are commonly used approaches. The transparency of distributed ledgers enhances integrity and accountability, but may pose privacy risks. Consequently, zero-knowledge proofs, homomorphic encryption and private transactions are employed. The PoW mechanism offers high security and decentralisation, but has limitations in terms of transaction capacity, latency and requires a lot of energy, whilst PoS and PBFT are more efficient, with different decentralisation characteristics. This has highlighted the exchanges between security, privacy, performance, decentralisation and energy efficiency.

Blockchain can mitigate threats such as data manipulation, forgery, document misuse and single points of failure through its distributed ledger. The integration of AI and ensemble models supports the detection of suspicious activity, whilst digital wallet-based authentication reduces the risk of brute-force

attacks, phishing, account takeovers and credential leaks. Homomorphic encryption, zero-knowledge proofs and trajectory obfuscation also strengthen privacy protection. However, blockchain does not entirely eliminate vulnerabilities in applications, identities and networks.

Table 3. Comparative analysis of the NIST and blockchain security approaches

No	NIST function	Blockchain features	Contribution to digital transaction security
1	Identify	Distributed ledger	Supports digital asset identification and transaction traceability
2	Protect	Cryptography, consensus mechanism, decentralization	Ensures confidentiality, integrity, authentication, and resistance to data manipulation
3	Detect	Immutable ledger, audit trail	Facilitates transaction verification and detection of unauthorized modifications.
4	Respond	Smart contracts	Automates predefined security actions, such as transaction validation.
5	Recover	Distributed ledger	Improving data availability through distributed node replication.

The application of blockchain in digital transaction security spans a range of disciplines. In the field of electrical engineering, blockchain supports peer-to-peer energy transactions and transaction integrity. In terms of the IoT, blockchain is used for device authentication, identity management and software updates. In control engineering, blockchain supports secure logging, auditing and anomaly detection in industrial and cyber-physical systems. In telecommunications, blockchain supports decentralised authentication, IoT identity management and the logging of network activity. Meanwhile, in computing and information systems, blockchain is applied to digital payments, digital identities, cloud computing and distributed data storage to enhance security and reduce single points of failure [9]. The differences in focus indicate that the implementation of blockchain is tailored to the security requirements of each domain.

The ways in which blockchain is applied to digital transaction security can be classified into three main categories. Firstly, blockchain functions as a security layer to verify and safeguard the integrity of transactions, particularly within digital payment systems. Secondly, blockchain is implemented as an identity management system through decentralised authentication mechanisms, such as SSI. Thirdly, blockchain is utilised as an audit system by providing an immutable record of transactions, which supports transparency and accountability in financial audits.

The findings of this research have practical implications for the development of digital transaction security. In the banking sector, consensus, immutable ledgers and smart contracts can enhance integrity, efficiency and fraud prevention. Whilst in the telecommunications sector they support infrastructure management, asset monitoring and secure activity logging. For practitioners, the choice of platform, consensus mechanism and architecture must be tailored to requirements regarding security, privacy, transaction volume and performance. Hybrid approaches and the integration of AI can provide solutions for maintaining data integrity and improving fraud detection. Their implementation also requires clear regulation and governance, as well as more efficient consensus mechanisms to enhance scalability.

4. CONCLUSION

According to a SLR of 100 articles, blockchain has the ability to improve the security of digitized transactions through cryptography, decentralised consensus and a distributed ledger. These mechanisms improve data integrity, transaction transparency and transaction reliability. However, its implementation still faces challenges relating to scalability, energy consumption and the complexity of integration with existing digital transaction systems. A hybrid architecture that combines conventional databases with blockchain offers a realistic approach to balancing security and efficiency. This study has limitations relating to the scope of the database and the review methodology, particularly the selection criteria and differences in study characteristics, which may affect the completeness and generalisability of the results. Further research should broaden the database and the search period, empirically compare platforms and consensus mechanisms, and develop consensus algorithms that are more energy-efficient and scalable, as well as enhance privacy protection and smart contract security. The integration of AI to detect threats also presents a research opportunity. With technological innovation and appropriate governance, blockchain has the potential to strengthen security and trust within the digital transaction ecosystem.

FUNDING INFORMATION

No governmental, commercial, or non-profit agency funded this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ni Komang Dewi Mahayani	✓	✓		✓	✓	✓		✓	✓	✓			✓	
Yadhurani Dewi Amritha		✓						✓		✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The author declares that there are no competing financial interests or conflicts of interest that could influence, or be perceived to influence, the results of this research.

DATA AVAILABILITY

No new data were produced or processed in this research, hence data availability is irrelevant.

REFERENCES

[1] C. H. Tsai, D. K. Liou, and H. L. Lee, "Blockchain-supported online banking scheme," *Egyptian Informatics Journal*, vol. 27, no. March 2023, 2024, doi: 10.1016/j.eij.2024.100516.

[2] Z. Mastilo, F. Barić, and A. Puška, "Challenges and Opportunities of Implementing Digital Payment Systems in Southeast European Countries," *Journal of Central Banking Theory and Practice*, vol. 14, no. 2, pp. 5–28, 2025, doi: 10.2478/jcbtp-2025-0011.

[3] A. Alenizi, S. Mishra, and A. Baihan, "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Engineering Journal*, vol. 15, no. 6, p. 102733, 2024, doi: 10.1016/j.asej.2024.102733.

[4] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, 2022, doi: 10.1016/j.bcra.2022.100067.

[5] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decision Analytics Journal*, vol. 9, p. 100344, 2023, doi: 10.1016/j.dajour.2023.100344.

[6] A. Rustam, N. Hasanah, H. Pasaribu, Q. Aina, and L. Judijanto, "The Role of Blockchain Technology in Increasing Transparency and Security of Financial Management in the Banking Sector," *Journal of Ecohumanism*, vol. 4, no. 1, pp. 5290–5301, 2025, doi: 10.62754/joe.v4i1.6463.

[7] N. Shehata and R. D'Souza, "Conducting a High-Quality Systematic Review," *Journal of Rheumatology*, vol. 52, no. 7, pp. 636–646, 2025, doi: 10.3899/jrheum.2024-1241.

[8] D. Al-Eisawi, "A Design Framework for Novice Using Grounded Theory Methodology and Coding in Qualitative Research: Organisational Absorptive Capacity and Knowledge Management," *International Journal of Qualitative Methods*, vol. 21, pp. 1–13, 2022, doi: 10.1177/16094069221113551.

[9] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Future Internet*, vol. 14, no. 11, pp. 1–22, 2022, doi: 10.3390/fi14110341.

[10] H. Wei and Y. Zhang, "Research on the digital transaction model of the sports industry chain based on blockchain technology," *Scientific Reports*, vol. 15, no. 1, pp. 1–20, 2025, doi: 10.1038/s41598-025-10045-7.

[11] S. Kayikci and T. M. Khoshgoftaar, "Blockchain meets machine learning: a survey," *Journal of Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-023-00852-y.

[12] R. Yang, "Development and Supervision of Financial Technology Based on Blockchain," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/2615153.

[13] H. Louati *et al.*, "Adopting Artificial Intelligence to Strengthen Legal Safeguards in Blockchain Smart Contracts: A Strategy to Mitigate Fraud and Enhance Digital Transaction Security," *Journal of Theoretical and Applied Electronic Commerce Research* , vol. 19, no. 3, pp. 2139–2156, 2024, doi: 10.3390/jtaer19030104.

[14] A. Ferone and S. Verrilli, "Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency," *Future Internet*, vol. 17, no. 1, 2025, doi: 10.3390/fi17010031.

[15] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, "Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis," *Information Systems Frontiers*, vol. 25, no. 2, pp. 871–896, 2023, doi: 10.1007/s10796-022-10279-0.

[16] L. Jiang, "The use of blockchain technology in enterprise financial accounting information sharing," *PLoS ONE*, vol. 19, no. 2 February, 2024, doi: 10.1371/journal.pone.0298210.

[17] T. Alexander, "Integrating Blockchain Technology into Traditional Point of Sale (POS) Software to Secure Transactions," *Engineering: Open Access*, vol. 1, no. 1, pp. 01–11, 2023, doi: 10.33140/eoa.01.01.10.

[18] X. Zheng, "Research on blockchain smart contract technology based on resistance to quantum computing attacks," *PLoS ONE*, vol. 19, no. 5 May, pp. 1–22, 2024, doi: 10.1371/journal.pone.0302325.

[19] O. Prokopenko, A. Koldovskiy, M. Khalilova, A. Orazbayeva, and J. Machado, "Development of Blockchain Technology in Financial

Accounting," *Computation*, vol. 12, no. 12, pp. 1–19, 2024, doi: 10.3390/computation12120250.
[20] W. Chen, D. Botchie, A. Braganza, and H. Han, "A transaction cost perspective on blockchain governance in global value chains," *Strategic Change*, vol. 31, no. 1, pp. 75–87, 2022, doi: 10.1002/jsc.2487.
[21] Z. Zilin, K. T. Jing, H. C. Yee, D. Zihao, and L. Yao, "Blockchain Technology in Construction Supply Chain Management: Enhance Transaction Speed, Cost Effectiveness And Security," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 32, no. 3, pp. 400–420, 2023, doi: 10.37934/araset.32.3.400420.
[22] H. Taherdoost, "Blockchain Technology and Artificial Intelligence Together: A Critical Review on Applications," *Applied Sciences (Switzerland)*, vol. 12, no. 24, 2022, doi: 10.3390/app122412948.
[23] L. Hang, B. H. Kim, and D. H. Kim, "A Transaction Traffic Control Approach Based on Fuzzy Logic to Improve Hyperledger Fabric Performance," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/2032165.
[24] N. Y. Lee, "Cost-Effective and Reliable Sidechain Approach for Managing Small-Scale Digital Asset Trading Platforms," *Applied Sciences (Switzerland)*, vol. 15, no. 9, 2025, doi: 10.3390/app15095221.
[25] H. Y. Lin, "A secure transaction and smart contract architecture for internet of vehicles," *Science Progress*, vol. 107, no. 4, pp. 1–28, 2024, doi: 10.1177/00368504241296039.
[26] K. A. M. Ahmed, S. F. Saraya, J. F. Wanis, and A. M. T. Ali-Eldin, "A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards," *Future Internet*, vol. 15, no. 6, 2023, doi: 10.3390/fi15060208.
[27] S. Huang, "Optimization of intelligent financial management system based on blockchain and internet of things," *Scientific Reports*, vol. 15, no. 1, pp. 1–14, 2025, doi: 10.1038/s41598-025-12217-x.
[28] H. Liu *et al.*, "A Financial Management Platform Based on the Integration of Blockchain and Supply Chain," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031497.
[29] J. Jiang and J. Chen, "Framework of blockchain-supported e-commerce platform for small and medium enterprises," *Sustainability (Switzerland)*, vol. 13, no. 15, 2021, doi: 10.3390/su13158158.
[30] Y. Liu, S. Zhang, M. Chen, Y. Wu, and Z. Chen, "The sustainable development of financial topic detection and trend prediction by data mining," *Sustainability (Switzerland)*, vol. 13, no. 14, pp. 1–19, 2021, doi: 10.3390/su13147585.
[31] S. Hegde, G. Aishwarya, A. Hugar, and V. B. Suneeta, "Bank Management System Using Blockchain Technology," *Lecture Notes in Networks and Systems*, vol. 401, no. 7, pp. 209–218, 2023, doi: 10.1007/978-981-19-0098-3_22.
[32] M. Sun, "The Application of Embedded Hardware System and Blockchain in Rural Financial Management Cloud Platform," *Decision Making: Applications in Management and Engineering*, vol. 7, no. 2, pp. 81–100, 2024, doi: 10.31181/dmame7220241040.
[33] R. V. Anand *et al.*, "Design of an improved model using federated learning and LSTM autoencoders for secure and transparent blockchain network transactions," *Scientific Reports*, vol. 15, no. 1, pp. 1–18, 2025, doi: 10.1038/s41598-024-83564-4.
[34] H. Rabbani *et al.*, "Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech," *PeerJ Computer Science*, vol. 10, pp. 1–38, 2024, doi: 10.7717/peerj-cs.2280.
[35] C. McCabe, A. I. C. Mohideen, and R. Singh, "A Blockchain-Based Authentication Mechanism for Enhanced Security," *Sensors*, vol. 24, no. 17, 2024, doi: 10.3390/s24175830.
[36] S. Peng, L. Zhu, S. Hu, Z. Cai, and W. Liu, "Enhancing Global Blockchain Privacy via a Digital Mutual Trust Mechanism," *Mathematics*, vol. 12, no. 10, pp. 1–20, 2024, doi: 10.3390/math12101481.
[37] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology," *Simulation Modelling Practice and Theory*, vol. 138, 2025, doi: 10.1016/j.simpat.2024.103027.
[38] M. Sadiq, A. F. Aysan, and U. N. Kayani, "Digital currency and blockchain security in accelerating financial stability: A mediating role of credit supply," *Borsa Istanbul Review*, vol. 23, no. 6, pp. 1251–1262, 2023, doi: 10.1016/j.bir.2023.09.009.
[39] S. Negi, "A blockchain technology for improving financial flows in humanitarian supply chains: benefits and challenges," *Journal of Humanitarian Logistics and Supply Chain Management*, vol. 15, no. 2, pp. 154–174, 2025, doi: 10.1108/JHLSCM-10-2023-0099.
[40] H. Louati, A. Louati, E. Kariri, and A. Almekhlafi, "AI-Based Anomaly Detection and Optimization Framework for Blockchain Smart Contracts," *Administrative Sciences*, vol. 15, no. 5, pp. 1–19, 2025, doi: 10.3390/admsci15050163.
[41] A. Panigrahi *et al.*, "Enhancing blockchain transaction classification with ensemble learning approaches," *Scientific Reports*, vol. 15, no. 1, pp. 1–30, 2025, doi: 10.1038/s41598-025-04072-7.
[42] A. Vdovichen, Y. Koroliuk, O. Vdovichena, I. Losheniuk, and N. Shuprudko, "The use of blockchain technology for managing digital assets in marketing management," *Periodicals of Engineering and Natural Sciences*, vol. 13, no. 1, pp. 295–304, 2025, doi: 10.21533/pen.v13.i1.305.
[43] Z. Feng, Y. Li, and X. Ma, "Blockchain-oriented approach for detecting cyber-attack transactions," *Financial Innovation*, vol. 9, no. 1, 2023, doi: 10.1186/s40854-023-00490-6.
[44] A. Upadhyay, S. Mukhuty, V. Kumar, and Y. Kazancoglu, "Blockchain technology and the circular economy: Implications for sustainability and social responsibility," *Journal of Cleaner Production*, vol. 293, p. 6, 2021, doi: 10.1016/j.jclepro.2021.126130.
[45] E. Abad-Segura, A. Infante-Moro, M. D. González-Zamar, and E. López-Meneses, "Blockchain technology for secure accounting management: Research trends analysis," *Mathematics*, vol. 9, no. 14, pp. 1–26, 2021, doi: 10.3390/math9141631.
[46] Y. Li, Y. Gong, M. Wu, Y. Li, and W. Wang, "Applications of blockchain technologies in artificial electricity market settlement and clearing," *International Journal of Low-Carbon Technologies*, vol. 19, no. June, pp. 2153–2161, 2024, doi: 10.1093/ijlct/ctae174.
[47] Z. Gu and O. Dib, "Enhancing fraud detection in the Ethereum blockchain using ensemble learning," *PeerJ Computer Science*, vol. 11, 2025, doi: 10.7717/PEERJ-CS.2716.
[48] H. Jamshed, U. Waheed, S. Iqbal, M. Faheem, M. W. Ashraf, and Y. Mansoor, "Dynamic smart contracts framework on Ethereum private blockchain for real estate management," *The Journal of Engineering*, vol. 2025, no. 1, pp. 1–19, 2025, doi: 10.1049/tje2.70063.
[49] Y. Ren, Y. Ren, H. Tian, W. Song, and Y. Yang, "Improving transaction safety via anti-fraud protection based on blockchain," *Connection Science*, vol. 35, no. 1, 2023, doi: 10.1080/09540091.2022.2163983.
[50] K. Chen, L.-F. Lee, W. Chiu, C. Su, K.-H. Yeh, and H.-C. Chao, "A Trusted Reputation Management Scheme for Cross-Chain Transactions," *Sensors*, vol. 23, no. 13, p. 6033, Jun. 2023, doi: 10.3390/s23136033.
[51] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors*, vol. 21, no. 4, pp. 1–17, 2021, doi: 10.3390/s21041540.
[52] X. Xia, T. Hou, X. Liu, C. Zong, and S. Mu, "Protecting Check-In Data Privacy in Blockchain Transactions with Preserving High Trajectory Pattern Utility," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/9358531.
[53] F. M. Xin and M. S. N. M. Radzi, "Application and prospect analysis of blockchain technology in intellectual property protection of e-commerce," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 10, pp. 1–15, 2024, doi: 10.24294/jipd.v8i10.7113.
[54] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, and F. Ali, "Role of authentication factors in Fin-tech mobile transaction

security," *Journal of Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00807-3.
[55] N. Dashkevich, S. Counsell, and G. Destefanis, "Blockchain Financial Statements: Innovating Financial Reporting, Accounting, and Liquidity Management," *Future Internet*, vol. 16, no. 7, 2024, doi: 10.3390/fi16070244.
[56] K. H. Yeh, G. Y. Yang, C. Butpheng, L. F. Lee, and Y. H. Liu, "A Secure Interoperability Management Scheme for Cross-Blockchain Transactions," *Symmetry*, vol. 14, no. 12, pp. 1–19, 2022, doi: 10.3390/sym14122473.
[57] Y. Mezquita, A. B. Gil-González, A. M. D. Rey, J. Prieto, and J. M. Corchado, "Towards a Blockchain-Based Peer-to-Peer Energy Marketplace," *Energies*, vol. 15, no. 9, pp. 1–20, 2022, doi: 10.3390/en15093046.
[58] Z. Wei *et al.*, "Privacy Protection Method for Blockchain Transactions Based on the Stealth Address and the Note Mechanism," *Applied Sciences (Switzerland)*, vol. 14, no. 4, 2024, doi: 10.3390/app14041642.
[59] A. S. M. T. Hasan, S. Sabah, R. U. Haque, A. Daria, A. Rasool, and Q. Jiang, "Towards Convergence of IoT and Blockchain for Secure Supply Chain Transaction," *Symmetry*, vol. 14, no. 1, pp. 1–19, 2022, doi: 10.3390/sym14010064.
[60] S. Yao and D. Zhang, "A blockchain-based privacy-preserving transaction scheme with public verification and reliable audit," *Electronic Research Archive*, vol. 31, no. 2, pp. 729–753, 2023, doi: 10.3934/era.2023036.
[61] B. M. Yakubu, J. Sabi'u, and P. Bhattarakosol, "Blockchain-based privacy and security model for transactional data in large private networks," *Scientific Reports*, vol. 13, no. 1, pp. 1–11, 2023, doi: 10.1038/s41598-023-44101-x.
[62] X. Liang, W. Ruan, Z. Xu, and J. Liu, "Analysis of Safe Storage of Network Information Data and Financial Risks Under Blockchain Combined With Edge Computing," *Journal of Global Information Management*, vol. 30, no. 11, pp. 3095–3114, 2022, doi: 10.4018/JGIM.312580.
[63] W. Zhou, D. Zhang, G. Han, W. Zhu, and X. Wang, "A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT," *Applied Sciences (Switzerland)*, vol. 13, no. 22, 2023, doi: 10.3390/app132212389.
[64] W. Wang, G. Chen, C. Chu, and W. Lan, "A Blockchain-Based Continuous Micropayment Scheme Using Lockable Signature," *Mathematics*, vol. 11, no. 16, pp. 1–18, 2023, doi: 10.3390/math11163472.
[65] T. V. Daugaard, J. B. Jensen, R. J. Kauffman, and K. Kim, "Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering," *Electronic Commerce Research and Applications*, vol. 65, no. February, p. 101386, 2024, doi: 10.1016/j.elerap.2024.101386.
[66] A. Thommandru and D. B. Chakka, "Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks," *Sustainable Futures*, vol. 5, no. February, p. 100107, 2023, doi: 10.1016/j.sftr.2023.100107.
[67] C. Yi, J. Liu, S. Wan, J. Fang, B. Sun, and L. Zhang, "Data Deduplication Based on Content Locality of Transactions to Enhance Blockchain Scalability," *ACM Transactions on Architecture and Code Optimization*, vol. 21, no. 4, 2024, doi: 10.1145/3680547.
[68] Z. Xue, M. Wang, Q. Zhang, Y. Zhang, and P. Liu, "A regulatable blockchain transaction model with privacy protection," *International Journal of Computational Intelligence Systems*, vol. 14, no. 1, pp. 1642–1652, 2021, doi: 10.2991/ijcis.d.210528.001.
[69] A. K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. T. Ahmed, "Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0," *Sensors*, vol. 23, no. 2, 2023, doi: 10.3390/s23020947.
[70] J. H. Yi and J. Moon, "Secure and Transparent Craftwork Authentication and Transaction System: Integrating Digital Fingerprinting and Blockchain Technologies," *Applied Sciences (Switzerland)*, vol. 14, no. 19, 2024, doi: 10.3390/app14199054.
[71] K. M. Khan, J. Arshad, and M. M. Khan, "Empirical analysis of transaction malleability within blockchain-based e-Voting," *Computers and Security*, vol. 100, no. December, 2021, doi: 10.1016/j.cose.2020.102081.
[72] R. Xie and M. Tang, "A digital resource copyright protection scheme based on blockchain cross-chain technology," *Heliyon*, vol. 10, no. 17, p. e36830, 2024, doi: 10.1016/j.heliyon.2024.e36830.
[73] D. Yang, L. Zhao, F. Leng, and Z. Shi, "Design of knowledge transaction protection mechanism in the open innovation community based on blockchain technology," *Data Science and Management*, vol. 8, no. 1, pp. 86–93, 2025, doi: 10.1016/j.dsm.2024.08.002.
[74] X. Li, J. Zhang, H. Long, Y. Chen, and A. Zhang, "Optimization of Digital Information Management of Financial Services Based on Artificial Intelligence in the Digital Financial Environment," *Journal of Organizational and End User Computing*, vol. 35, no. 3, pp. 1–17, 2023, doi: 10.4018/JOEUC.318478.
[75] Z. Fu, P. Dong, S. Li, and Y. Ju, "An intelligent cross-border transaction system based on consortium blockchain: A case study in shenzhen, China," *PLoS ONE*, vol. 16, no. 6 June, pp. 1–22, 2021, doi: 10.1371/journal.pone.0252489.
[76] K. A. A. Mutlaq *et al.*, "Blockchain assisted signature and certificate based protocol for efficient data protection and transaction management in smart grids," *Plos One*, vol. 20, no. 5 May, pp. 1–32, 2025, doi: 10.1371/journal.pone.0318182.
[77] A. Zhao, "Financial Risk Evaluation of Digital Currency Based on CART Algorithm Blockchain," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/1356480.
[78] A. Boumaiza, "Advancing Sustainable Investment Efficiency and Transparency Through Blockchain-Driven Optimization," *Sustainability (Switzerland)*, vol. 17, no. 5, 2025, doi: 10.3390/su17052000.
[79] R. O. Ogundokun, M. O. Arowolo, R. Damaševičius, and S. Misra, "Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning," *Telecom*, vol. 4, no. 2, pp. 279–297, 2023, doi: 10.3390/telecom4020017.
[80] G. Lăzăroiu, M. Bogdan, M. Geamănu, L. Hurloiu, L. Ionescu, and R. Ștefănescu, "Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management," *Oeconomia Copernicana*, vol. 14, no. 3, pp. 707–730, 2023, doi: 10.24136/oc.2023.021.
[81] N. A. Saqib and S. T. AL-Talla, "Scaling Up Security and Efficiency in Financial Transactions and Blockchain Systems," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, 2023, doi: 10.3390/jsan12020031.
[82] Y. Jiang, G. Sun, and T. Feng, "Research on Data Transaction Security Based on Blockchain," *Information (Switzerland)*, vol. 13, no. 11, pp. 1–17, 2022, doi: 10.3390/info13110532.
[83] G. Sladić, B. Milosavljević, S. Nikolić, D. Sladić, and A. Radulović, "A blockchain solution for securing real property transactions: A case study for serbia," *ISPRS International Journal of Geo-Information*, vol. 10, no. 1, 2021, doi: 10.3390/ijgi10010035.
[84] X. Ma, Y. Li, and Z. Wu, "Design and Implementation of Digital Currency Transaction Security Mechanism Using Blockchain with Hybrid PoW+PoS Consensus and Multi-Signature Privacy Protection," *Informatica (Slovenia)*, vol. 49, no. 5, pp. 109–122, 2025, doi: 10.31449/inf.v49i5.7101.
[85] S. Bhatnagar, M. Dayal, D. Singh, S. Upreti, K. Upreti, and J. Kumar, "Block-Hash Signature (BHS) for Transaction Validation in Smart Contracts for Security and Privacy using Blockchain," *Journal of Mobile Multimedia*, vol. 19, no. 4, pp. 935–962, 2023, doi: 10.13052/jmm1550-4646.1941.
[86] M. Kowalski, Z. W. Y. Lee, and T. K. H. Chan, "Blockchain technology and trust relationships in trade finance," *Technological Forecasting and Social Change*, vol. 166, pp. 29–43, 2021, doi: 10.1016/j.techfore.2021.120641.
[87] W. Xu, D. Hu, K. R. Lang, and J. L. Zhao, "Blockchain and digital finance," *Financial Innovation*, vol. 8, no. 1, 2022, doi: 10.1186/s40854-022-00420-y.
[88] S. Asaithambi, L. Ravi, M. Devarajan, A. S. Almazyad, G. Xiong, and A. W. Mohamed, "Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs," *Egyptian Informatics Journal*, vol. 25, no. January,

p. 100444, 2024, doi: 10.1016/j.eij.2024.100444.
[89] T. Norbu, J. Y. Park, K. W. Wong, and H. Cui, "Understanding Consumer Acceptance for Blockchain-Based Digital Payment Systems in Bhutan," *Future Internet*, vol. 17, no. 4, pp. 1–25, 2025, doi: 10.3390/fi17040134.
[90] A. Sharma, S. S. Bhanawat, and R. B. Sharma, "Adoption of Blockchain Technology Based Accounting Platform," *Academic Journal of Interdisciplinary Studies*, vol. 11, no. 2, pp. 155–162, 2022, doi: 10.36941/ajis-2022-0042.
[91] S. Abdallah-Ou-Moussa, M. Wynn, and O. Kharbouch, "Blockchain, Cryptocurrencies, and Decentralized Finance: A Case Study of Financial Inclusion in Morocco," *International Journal of Financial Studies*, vol. 13, no. 3, pp. 1–25, 2025, doi: 10.3390/ijfs13030124.
[92] H. A. Al-Khawaja, "Studying the mediating role of blockchain on the impact of the use of financial technology (FinTech) on the competitive advantage of banks," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 9, pp. 1–21, 2024, doi: 10.24294/jipd.v8i9.6477.
[93] Z. Yang, S. Ali, W. Tao, and H. Chen, "From Transactions to Transformation: Exploring the Impact of Blockchain on Customer Financial Well-being," *SAGE Open*, vol. 14, no. 2, pp. 1–18, 2024, doi: 10.1177/21582440241253955.
[94] R. K. Jena, "Examining the Factors Affecting the Adoption of Blockchain Technology in the Banking Sector: An Extended UTAUT Model," *International Journal of Financial Studies*, vol. 10, no. 4, 2022, doi: 10.3390/ijfs10040090.
[95] S. Nanayakkara, S. Perera, S. Senaratne, G. T. Weerasuriya, and H. M. N. D. Bandara, "Blockchain and smart contracts: A solution for payment issues in construction supply chains," *Informatics*, vol. 8, no. 2, pp. 1–16, 2021, doi: 10.3390/informatics8020036.
[96] A. Ogunrinde, C. De-Pablos-Heredero, J.-L. Montes-Botella, and L. Fernández-Sanz, "The Impact of Blockchain Technology and Dynamic Capabilities on Banks' Performance," *Big Data and Cognitive Computing*, vol. 9, no. 6, p. 144, May 2025, doi: 10.3390/bdcc9060144.
[97] A. O. J. Kwok and H. Treiblmaier, "Blockchain technology as a driver of economic development in small economies: a dynamic capabilities framework," *Journal of Decision Systems*, vol. 33, no. 3, pp. 413–438, 2024, doi: 10.1080/12460125.2023.2214304.
[98] V. Kumari, P. K. Bala, and S. Chakraborty, "An Empirical Study of User Adoption of Cryptocurrency Using Blockchain Technology: Analysing Role of Success Factors like Technology Awareness and Financial Literacy," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 18, no. 3, pp. 1580–1600, 2023, doi: 10.3390/jtaer18030080.
[99] S. N. Ata, A. K. Hassan, H. S. Selim, B. E. Hammad, H. M. Abdelhalim, and A. M. Abdelhalim, "The Use of Blockchain Technology and Its Reflection in the Financial Performance of Investment Projects Developed by the Ministry of Sports," *Economies*, vol. 11, no. 5, 2023, doi: 10.3390/economies11050140.
[100] J. Du, Y. Shi, W. Li, and Y. Chen, "Can blockchain technology be effectively integrated into the real economy? Evidence from corporate investment efficiency," *China Journal of Accounting Research*, vol. 16, no. 2, p. 100292, 2023, doi: 10.1016/j.cjar.2023.100292.
[101] C. Viano, S. Avanzo, M. Cerutti, A. Cordero, C. Schifanella, and G. Boella, "Blockchain tools for socio-economic interactions in local communities," *Policy and Society*, vol. 41, no. 3, pp. 373–385, 2022, doi: 10.1093/polsoc/puac007.
[102] P. Garg, B. Gupta, K. N. Kapil, U. Sivarajah, and S. Gupta, "Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector," *Annals of Operations Research*, vol. 348, no. 3, pp. 1513–1546, 2025, doi: 10.1007/s10479-023-05254-0.
[103] T. Hakkarainen, A. Colicev, and T. Pedersen, "A perspective on three trade-offs of blockchain technology for the global strategy of the MNC," *Global Strategy Journal*, vol. 14, no. 3, pp. 635–654, 2024, doi: 10.1002/gsj.1509.

BIOGRAPHIES OF AUTHORS



Ni Komang Dewi Mahayani is currently pursuing higher education at the National Education University with an interest in developing academic competencies and research in her field. During her studies, she has been actively deepening her theoretical knowledge and practical skills to support her future professional career development. She can be contacted at email: dewimahayani94@gmail.com.



Yadhurani Dewi Amritha is a lecturer in the Information Technology Study Programme at the National Education University, specialising in statistics and data modelling, particularly longitudinal data using the Hidden Markov method. She obtained her Bachelor's degree in Mathematics from Yogyakarta State University (2020) and her Master's degree in Statistics from Gadjah Mada University (2023). Her experience includes teaching courses in data science, discrete mathematics, digital systems and data, it services management, calculus, and linear algebra, along with a background as a mathematics tutor at various levels and a claims division staff member at AJB Bumiputera. She is actively involved in organisations such as KMHD UNY, the UGM Postgraduate Mathematics Student Association, and various major committees in Yogyakarta and Bali. She is proficient in using Matlab, SPSS, SmartPLS, R, and Geogebra, holds certifications in language and data analytics, and is committed to advancing education and research in the fields of statistics, data science, and information technology. She can be contacted at email: Yadhurani@undiknas.ac.id.