Blockchain Frontier Technology (B-Front)
Vol. 6, No. 1, July, 2026, pp. 50∼61
E-ISSN: 2808-0009 | P-ISSN: 2808-0831, DOI: 10.34306

Implementation of Blockchain Technology to Enhance the Security of Online Payment Transactions

Ariesya Aprillia[1*], Denok Wahyudi Setyo Rahayu[2], Arista Ratih[3], Thomas Green[4]
[1]Faculty of Digital Business and Law, Maranatha Christian University, Indonesia
[2]Faculty of Economics, Islam Balitar University, Indonesia
[3]Faculty of Mathematics and Natural Sciences, Universitas Negeri Padang, Indonesia
[4]Department of Science and Technology, Eesp Incorporation, Samudra Hindia Britania
[1]ariesya.aprillia@eco.maranatha.edu, [2]denokwahyudisr@unisbablitar.ac.id, [3]aristaratih92@gmail.com, [4]thom.green@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission, 24-12-2025
Revised, 24-02-2026
Accepted, 30-03-2026
Published, 17-04-2026

Keywords:

Blockchain
Transparency
Payment Security
Digital Financial
Smart Contracts

ABSTRACT

The rapid growth of digital financial services has significantly increased the volume of online payment transactions, while simultaneously intensifying concerns related to transaction security, data integrity, privacy protection, and fraud due to the limitations of centralized payment architectures, which remain vulnerable to cyberattacks, data manipulation, and single points of failure. **This study aims** to analyze the role of blockchain technology in enhancing the security of online payment transactions by examining its core characteristics, including decentralization, transparency, immutability, and smart contracts. **This research** adopts a conceptual and descriptive comparative approach by synthesizing recent peer-reviewed literature to evaluate blockchain-based payment systems in comparison with conventional centralized systems. **The findings indicate** that blockchain implementation improves transaction security by reducing fraud risks, eliminating single points of failure, ensuring tamper-resistant records, and enhancing transparency and traceability, thereby increasing user trust. **These improvements contribute** to more reliable, transparent, and resilient digital payment infrastructures. Furthermore, blockchain technology supports the SDGs 8 (Decent Work and Economic Growth), SDGs 9 (Industry, Innovation, and Infrastructure), and SDGs 16 (Peace, Justice, and Strong Institutions), by promoting transparency, accountability, and long-term stability in digital financial ecosystems.

1. INTRODUCTION

The rapid expansion of digital financial services has transformed global payment ecosystems through technologies such as mobile banking, electronic wallets, and digital payment gateways [1]. These platforms improve efficiency, accessibility, and convenience for individuals and businesses, but they also introduce security risks, including data breaches, identity theft, payment fraud, and unauthorized access. Most traditional online payment systems rely on centralized architectures, which create single points of failure and increase vulnerability to cyberattacks. As digital transactions continue to grow in volume and cross-border reach, ensuring transaction security, integrity, and reliability has become a critical concern for financial institutions, regulators, and technology providers [2].

Blockchain technology has emerged as a potential solution to enhance online payment security through a decentralized and distributed ledger that records transactions transparently and immutably. By using cryptographic hashing, consensus mechanisms, and smart contracts, blockchain secures transaction validation, prevents data manipulation, and reduces risks such as fraud and double spending [3]. However, despite these advantages, blockchain implementation still faces challenges related to scalability, interoperability, regulatory compliance, and practical adoption. In particular, scalability remains a major limitation, as many public blockchain networks process transactions at lower speeds than centralized systems, potentially causing delays and higher costs in high-volume payment environments [4].

Beyond its technical benefits, blockchain implementation in online payment systems also aligns with the United Nations Sustainable Development Goals (SDGs). Secure blockchain-based payment infrastructures support SDG 9 by promoting resilient digital financial systems and SDG 16 by strengthening transparency and accountability in financial transactions [5]. In addition, secure digital payments contribute to SDG 8 by enabling safer and more efficient economic activities within the digital economy. Real-world implementations such as Bitcoin and Ethereum demonstrate how decentralized transaction verification and smart contracts can enhance transparency, prevent double spending, and create tamper-resistant financial records, thereby supporting the development of secure and trustworthy online payment ecosystems [6].

2. LITERATURE REVIEW

This chapter reviews relevant theories and recent scholarly discussions on blockchain technology and its role in enhancing the security of online payment transactions. The review focuses on blockchain security foundations, implementation in payment systems, associated risks, and empirical evidence, while highlighting links to sustainable digital infrastructure aligned with the United Nations SDGs.

2.1. Blockchain Technology and Security Foundations

Blockchain technology is widely recognized as a decentralized digital ledger that enhances transaction security through cryptographic mechanisms and distributed validation [7]. Unlike centralized payment systems, blockchain distributes transaction records across multiple network nodes, reducing dependence on a single authority and minimizing systemic vulnerabilities or single points of failure, thereby improving the reliability of digital financial transactions [8]. Security in blockchain is maintained through cryptographic hashing and digital signatures, which ensure data integrity, authenticity, and non-repudiation by generating unique hash values for transactions and verifying user identities through asymmetric cryptography [9]. In addition, blockchain networks use consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions across distributed nodes, ensuring that only legitimate transactions are recorded on the ledger [10].

Once validated, transactions become immutable and form a transparent audit trail within Distributed Ledger Technology (DLT), where identical copies of the ledger are maintained across multiple nodes and blocks are linked through cryptographic hashes, creating a secure chronological chain of records that supports SDG 9 and SDG 16 by strengthening resilient financial systems and promoting transparency in digital transactions [11].

2.2. Blockchain Implementation in Online Payment Systems

The implementation of blockchain technology in online payment systems has gained increasing attention as a solution to security, efficiency, and trust challenges [12]. Blockchain-based payment systems enable peer-to-peer transactions without centralized intermediaries, reducing transaction costs and operational complexity. The use of distributed ledger systems improves transaction traceability and verification accuracy, significantly lowering risks such as double spending and unauthorized transaction modification. In practice, blockchain is often deployed through permissioned or hybrid networks to balance decentralization with regulatory compliance, as full replacement of centralized payment infrastructure is rarely feasible in the short term [13].

Instead, hybrid integration models offer a more realistic transitional approach, where blockchain functions as a complementary verification and settlement layer while existing centralized systems continue to manage user authentication, transaction interfaces, and regulatory reporting [14]. Integration can be achieved through application programming interfaces (APIs), middleware solutions, and permissioned blockchain networks that allow controlled access for financial institutions and regulators, enabling gradual migration without

disrupting established operational workflows. Furthermore, smart contracts enhance payment systems by automating transaction execution based on predefined rules, minimizing human error and manipulation [15]. These features contribute to more reliable and efficient payment processes and support SDG 8 (Decent Work and Economic Growth) by strengthening trust in digital financial services and enabling broader participation in the digital economy [16].

Table 1. Blockchain Features in Online Payment Systems

Feature	**Role in Payment Systems**
Decentralization	Reduces single points of failure
Transparency	Enhances transaction traceability
Immutability	Prevents data manipulation
Smart Contracts	Automates secure payment execution

Table 1 shown summarizes the key blockchain features and their roles in enhancing online payment systems. Decentralization reduces reliance on a single authority, thereby minimizing single points of failure. Transparency improves transaction traceability and accountability, while immutability ensures that transaction records cannot be altered or manipulated. In addition, smart contracts automate payment execution securely, reducing human intervention and potential operational risks.

2.3. Security Risks and Limitations of Blockchain Based Payments

Despite its advantages, blockchain-based payment systems still face several security risks, particularly those related to smart contract vulnerabilities caused by coding errors or flawed logic [17]. Because smart contracts operate on immutable blockchain networks, errors cannot be easily corrected once deployed, increasing the impact of issues such as reentrancy attacks, integer overflows, and incorrect conditional logic. These weaknesses may lead to unauthorized transactions or financial losses. Therefore, rigorous code auditing, formal verification, and comprehensive security testing are essential before deployment [18]. Additional safeguards, such as upgradeable smart contracts and emergency pause mechanisms, can help mitigate risks, although blockchain systems remain vulnerable to external threats, including phishing attacks, compromised private keys, and insecure user interfaces.

Privacy, regulatory compliance, and scalability also present significant challenges in blockchain-based payment systems [19]. Public blockchain networks provide high transparency, but transaction data can be visible and traceable, potentially exposing sensitive information. This may conflict with data protection regulations such as the General Data Protection Regulation (GDPR), particularly the "right to be forgotten," which is difficult to implement due to blockchain immutability [20]. In addition, scalability is another major limitation, as blockchain networks require distributed validation across multiple nodes rather than relying on a single high-performance database, which can slow transaction processing and limit throughput. As a result, many public blockchain systems process fewer transactions per second than traditional payment networks [21]. To address this issue, solutions such as layer-two scaling mechanisms, off-chain payment channels, sharding techniques, and hybrid blockchain architectures have been developed. Although these approaches improve efficiency and transaction capacity, they also involve trade-offs related to complexity, cost, and security, making scalability a critical consideration in blockchain payment system design [22].

2.4. Empirical and Conceptual Evidence on Blockchain Payment Security

Recent empirical and conceptual studies consistently indicate that blockchain technology positively influences online payment security by reducing fraud and enhancing transaction integrity through decentralization, transparency, and immutability [23]. By distributing transaction records across multiple nodes, blockchain minimizes the risk of data manipulation and single points of failure, thereby improving system reliability and strengthening user trust through verifiable and secure transaction records [24]. These findings highlight the role of blockchain as a robust technological foundation for secure digital payment systems.

Furthermore, conceptual models emphasize blockchain's contribution to institutional accountability through immutable recordkeeping and enhanced auditability, as illustrated in Figure 1, which positions key blockchain dimensions as foundational constructs influencing transaction security, fraud prevention, and user trust. These improvements support sustainable digital finance and contribute to resilient financial infrastructure and inclusive economic growth, aligning with SDG 9 and SDG 8. However, further empirical validation is

still required across diverse regulatory and technological environments to strengthen the generalizability and practical applicability of these findings [25].

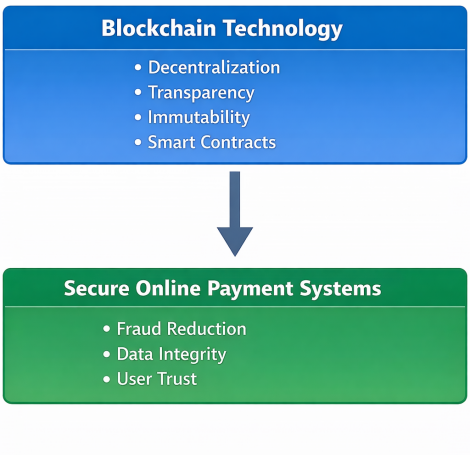

Figure 1. Conceptual Relationship Between Blockchain and Payment Security

The Figure 1 shown illustrates the conceptual relationship between blockchain technology and secure online payment systems, highlighting how decentralization, transparency, immutability, and smart contracts enhance payment security. These features reduce dependence on central authorities, prevent data manipulation, and automate transaction processes, thereby minimizing fraud. As a result, blockchain technology supports secure online payment systems by improving fraud reduction, ensuring data integrity, and increasing user trust.

3. RESEARCH METHODS

This section describes the methodological approach used to examine the relationship between blockchain technology characteristics and online payment transaction security. It outlines the research design, data collection procedures, and analysis techniques to ensure reliable and valid empirical findings.

3.1. Research Design and Approach

This study adopts a conceptual research design aimed at theory development and framework construction rather than empirical hypothesis testing [26]. The conceptual approach is appropriate given the emerging nature of blockchain applications in online payment security and the limited availability of standardized empirical datasets. By synthesizing existing theoretical perspectives and recent scholarly findings, this study develops a structured understanding of how blockchain technology enhances transaction security in digital payment systems [27].

The research emphasizes analytical reasoning and systematic interpretation of studies published after 2021, integrating key theories from information systems, cybersecurity, and financial technology literature to establish a coherent conceptual foundation [28]. This approach enables the identification of critical constructs, clarification of their relationships, and development of a theoretical framework to guide future empirical research. To strengthen its robustness and practical applicability, future studies are recommended to conduct empirical validation using quantitative and qualitative methods, such as Structural Equation Modeling (SEM) or Partial Least Squares (PLS-SEM), as well as pilot implementations in fintech environments to measure performance indicators including fraud reduction, transaction speed, system reliability, and user trust [29]. Overall, this conceptual design contributes to advancing academic discourse while providing strategic insights for secure and sustainable digital payment infrastructures.

3.2. Data Source and Literature Selection

The primary data source for this conceptual study consists of peer-reviewed journal articles, conference proceedings, and authoritative reports related to blockchain technology and online payment security [30]. Literature is selected based on relevance, publication quality, and recency, with a focus on studies published

from 2021 onward to ensure contemporary applicability. Priority is given to Scopus-indexed journals and publications from reputable academic publishers to maintain high standards of rigor and credibility. This approach ensures that the study draws on the most reliable and current evidence regarding blockchain features, security mechanisms, and digital payment systems [31].

The literature selection process follows a structured review procedure, including keyword identification, abstract screening, and detailed content analysis. Studies addressing blockchain implementation, security mechanisms, and digital payment infrastructures are systematically compared and synthesized. This method allows the identification of dominant themes, recurring constructs, and theoretical gaps, providing a clear conceptual foundation for model development [32]. The resulting conceptual synthesis not only informs the framework of this study but also ensures alignment with emerging trends in digital finance and global sustainability objectives, offering a structured basis for understanding how blockchain can enhance online payment security.

Table 2. Literature Selection Criteria

Criterion	**Description**
Publication period	$\geq$ 2021
Source type	Peer reviewed journals
Research focus	Blockchain, payment security

Table 2 shown summarizes the criteria used for selecting literature in this conceptual study. Only peer reviewed journal articles published from 2021 onward are included to ensure the relevance and currency of the discussion. The selected studies focus specifically on blockchain technology and online payment security and are sourced from Scopus-indexed journals or other reputable academic publishers to maintain high scholarly quality.

3.3. Conceptual Variables and Framework Development

This study conceptualizes blockchain implementation as a multidimensional construct comprising decentralization, transparency, immutability, and smart contract reliability. These dimensions, derived from recurring themes in recent literature, distinguish blockchain-based systems from traditional centralized payment infrastructures [33]. Decentralization reduces reliance on a single authority, enhancing network resilience, while transparency ensures transactions are verifiable and traceable. Immutability provides tamper-resistant records, and reliable smart contracts automate secure transactions, reducing human error and fraud. Collectively, these features strengthen online payment transaction security, defined as the ability to protect data, prevent fraud, and enhance user trust [34].

Through conceptual mapping, the study establishes relationships between blockchain dimensions and transaction security outcomes, illustrating how these attributes contribute to secure digital payments. While the framework does not empirically test causality, it offers a structured model explaining how blockchain enhances reliability, transparency, and accountability. This foundation supports future empirical research to validate the model and explore practical implications for financial institutions, regulators, and end-users, fostering more secure and resilient online payment systems [35].

Table 3. Conceptual Variables and Descriptions

Variable	**Dimension**	**Conceptual Role**
Blockchain Implementation	Decentralization	Eliminates single points of failure
-	Transparency	Improves traceability
-	Immutability	Ensures data integrity
-	Smart Contracts	Automates secure execution
Online Payment Security	Transaction Security	Fraud prevention and trust

Table 3 shown presents the conceptual constructs used in this study. Blockchain implementation is defined through decentralization, transparency, immutability, and smart contracts, which collectively support

secure and reliable payment processes. Online payment security focuses on transaction security, emphasizing fraud prevention and the enhancement of user trust.

3.4. Research Model and SDGs Alignment

This study proposes a conceptual research model that explains the relationship between blockchain implementation and online payment transaction security [36]. Blockchain implementation is conceptualized through key dimensions, including decentralization, transparency, immutability, and smart contract reliability, which collectively contribute to reducing fraud, ensuring data integrity, and increasing user trust in digital payment systems. The model provides a theoretical foundation for understanding how blockchain technology enhances transaction security without relying on empirical testing. More specifically, decentralization contributes to fraud reduction by eliminating single points of control that are vulnerable to manipulation or cyberattacks [37]. Immutability strengthens data integrity by ensuring that validated transaction records cannot be altered retroactively. Transparency enhances traceability, enabling transaction monitoring and auditability, which further reduces opportunistic behavior. Smart contracts improve procedural security by automating rule-based transaction execution, minimizing human error and discretionary intervention [38]. Collectively, these dimensions influence online payment security outcomes through interrelated mechanisms that reinforce system reliability, accountability, and user trust. The refined framework therefore emphasizes directional linkages between blockchain features and measurable security performance indicators [39].

In addition, the proposed model aligns with the United Nations SDGs 9 (Industry, Innovation, and Infrastructure) by supporting secure digital infrastructure, and SDGs 16 (Peace, Justice, and Strong Institutions) through improved transparency and accountability in financial transactions.

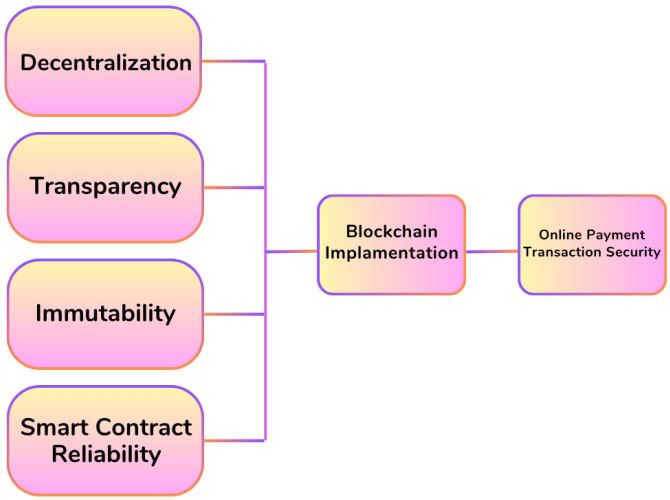

Figure 2. Conceptual Research Framework

The Figure 2 shown illustrates a conceptual research framework where decentralization, transparency, immutability, and smart contracts function as key components that support effective blockchain implementation. This implementation subsequently plays an important role in enhancing the security of online payment transactions by ensuring reliability and trustworthiness.

4. RESULTS AND DISCUSSION

This section discusses the theoretical findings of the study by synthesizing existing literature to explain how blockchain implementation enhances online payment security. The discussion highlights the role of decentralization, immutability, transparency, and smart contracts in reducing fraud, strengthening trust, and supporting sustainable digital finance aligned with the SDGs.

4.1. Conceptual Findings on Blockchain and Online Payment Security

As a conceptual study, the findings are presented as theoretical insights rather than empirical or statistical results. The analysis indicates that blockchain technology positively influences online payment security

by addressing key vulnerabilities in centralized systems [40]. Decentralization reduces single points of failure and lowers the risk of large-scale cyberattacks or system manipulation, while immutability protects transaction integrity by preventing unauthorized data modification. In addition, transparency improves traceability and accountability within digital payment processes. Smart contracts further strengthen security by automatically executing transactions based on predefined rules, reducing human intervention and the potential for fraud or error. Observations from existing blockchain networks support these insights. For instance, the Bitcoin network has demonstrated resilience through its distributed ledger that maintains transaction integrity across global nodes, while Ethereum-based payment applications enable programmable transactions that reduce reliance on third-party intermediaries. Although volatility and regulatory issues remain challenges, these implementations illustrate how blockchain architecture can improve transaction security, transparency, and reliability in digital payment environments [41].

Overall, these conceptual findings suggest that blockchain-based payment systems can enhance institutional trust and system reliability. From a sustainability perspective, improved transaction security supports inclusive and resilient digital financial ecosystems, aligning with SDGs 8 (Decent Work and Economic Growth) and SDGs 16 (Peace, Justice, and Strong Institutions). However, further empirical research is needed to measure the magnitude of blockchain's impact on transaction security and to examine factors such as regulatory environments, technological maturity, and user adoption that may influence its effectiveness [42].

4.2. Discussion of Blockchain Security Mechanisms in Digital Payments

This discussion explains how blockchain security mechanisms enhance the reliability of online payment systems. Unlike traditional centralized infrastructures, blockchain distributes validation across multiple nodes, improving fault tolerance and reducing vulnerability to cyberattacks, especially in high-volume and cross-border transactions. Smart contracts further strengthen security by automatically executing transactions based on predefined conditions, reducing human intervention and operational errors [43]. However, flawed code or malicious exploitation may increase risks, making safeguards such as independent audits, secure coding standards, runtime monitoring, and governance frameworks essential.

The effectiveness of blockchain security also depends on appropriate system architecture, governance structures, and regulatory alignment. Challenges such as smart contract vulnerabilities, privacy concerns, and the scalability security decentralization trade-off require careful system design to balance security and efficiency [44]. Public blockchains offer greater decentralization and transparency but may complicate regulatory compliance, while permissioned blockchains restrict validation to authorized participants, enabling stronger monitoring though introducing partial centralization. Therefore, financial institutions must evaluate whether public, private, or hybrid blockchain models best fit their transaction volume and regulatory requirements.

Beyond technical and governance aspects, practical challenges also affect blockchain adoption in online payment systems. Significant investment is needed for infrastructure development, cybersecurity auditing, smart contract verification, and workforce training. Integration with legacy banking systems requires interoperability frameworks, data migration strategies, and compatibility testing to avoid operational fragmentation [45]. Additionally, compliance with AML, KYC, and data protection regulations increases complexity, especially in cross-border payments. Therefore, successful implementation depends on technological capability, regulatory clarity, institutional readiness, and careful evaluation of costs and compliance requirements [46].

Table 4. Comparison of Centralized and Blockchain Based Payment

Aspect	**Centralized Systems**	**Blockchain Systems**
Control	Single authority	Distributed network
Security risk	High	Lower
Transparency	Limited	High

Table 4 shown compares centralized and blockchain based payment systems in control, security, and transparency. Centralized systems rely on a single authority, leading to higher security risks and limited transparency. Blockchain systems use a distributed network, reducing vulnerabilities and ensuring greater transparency, making them more secure and reliable for digital payments.

4.3. Blockchain, Institutional Trust, and SDGs Alignment

From a sustainability perspective, blockchain-based online payment systems contribute to broader socio-economic goals beyond technical security improvements. By improving transparency, accountability, and trust in financial transactions, blockchain supports SDGs 16 by strengthening governance and reducing fraud through tamper-resistant financial records [47]. At the same time, blockchain aligns with SDGs 9 by enabling innovative and resilient digital financial infrastructures, such as cross-border payment platforms that reduce settlement times from days to near real-time while maintaining verifiable audit trails. These systems also improve economic efficiency and institutional accountability by allowing financial institutions and regulators to monitor transactions more effectively and reduce financial misconduct [48].

In addition, blockchain can lower transaction costs for small and medium enterprises (SMEs), particularly in cross-border payments that typically involve multiple intermediaries, thereby encouraging fintech innovation and supporting resilient digital financial infrastructure [49]. Furthermore, blockchain supports SDGs 16 and SDGs 8 by strengthening transparency and encouraging broader participation in the digital economy. Immutable transaction records reduce opportunities for fraud and unauthorized manipulation, while blockchain-based monitoring systems enable regulators to detect suspicious activities more quickly. Increased trust in digital payments also encourages participation from small businesses, startups, and underserved communities, contributing to inclusive and sustainable economic growth [50].

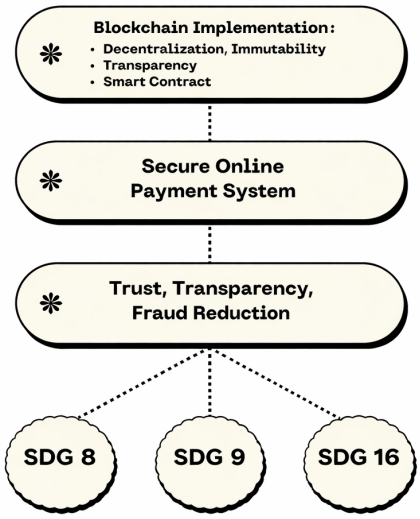

Figure 3. Conceptual Link between Blockchain, Payment Security, and SDGs

The Figure 3 shown illustrates the relationship between blockchain implementation and secure online payment systems. Core blockchain features decentralization, immutability, transparency, and smart contracts enhance transaction reliability, traceability, and fraud prevention. By improving trust and accountability in digital financial transactions, these mechanisms support the development of secure and transparent payment infrastructures, contributing to the achievement of SDGs 8, SDGs 9, and SDGs 16.

5. MANAGERIAL IMPLICATIONS

From a managerial perspective, this study provides strategic guidance for financial institutions, fintech companies, and policymakers seeking to enhance digital payment systems [51]. Blockchain can redesign payment infrastructures through decentralized validation, immutable records, and automated smart contracts that reduce operational risks, prevent fraud, and ensure consistent transaction processing. However, successful adoption also requires addressing human and cognitive barriers, particularly limited blockchain literacy among employees, decision-makers, and users [52]. Many stakeholders still associate blockchain only with cryptocurrency volatility, which can create resistance and reduce trust in decentralized payment systems. To address

this, financial institutions should incorporate structured educational initiatives such as technical training, compliance workshops, executive seminars, and user awareness programs that explain blockchain's role in fraud prevention, data integrity, and transaction transparency [53].

Beyond organizational readiness, supportive regulatory frameworks and collaboration among financial institutions, fintech firms, and policymakers are essential for successful blockchain implementation [54]. Clear guidelines on data privacy, transaction monitoring, and compliance standards can reduce regulatory uncertainty and encourage responsible innovation in digital payment systems. Although blockchain adoption requires significant investment, system integration, and governance adjustments, its implementation can strengthen payment security, transparency, and operational resilience [55]. In the long term, these improvements contribute to stronger financial ecosystems and support broader goals such as financial inclusion, economic growth, and improved institutional governance.

6. CONCLUSION

This conceptual paper contributes to the literature by presenting a theoretical framework explaining how blockchain technology enhances the security of online payment transactions. By synthesizing findings from recent studies, the paper highlights how blockchain's core attributes decentralization, immutability, transparency, and smart contracts help mitigate vulnerabilities commonly found in traditional centralized systems. These features reduce the risks of fraud, cyberattacks, and data manipulation while improving the reliability, consistency, and trustworthiness of digital payment processes.

Beyond security improvements, the study emphasizes blockchain's strategic role in supporting sustainable digital financial infrastructures. Blockchain-based payment systems can promote financial inclusion by expanding access to secure transactions, support economic growth through efficient and transparent payment mechanisms, and strengthen institutional governance through improved traceability and accountability. These contributions align with the SDGs. In practice, blockchain-based transaction monitoring can improve compliance transparency, enhance anti-fraud mechanisms, and support financial access for underserved populations. By increasing operational efficiency and auditability, blockchain payment infrastructures demonstrate their potential as a strategic enabler for sustainable economic development and institutional stability.

Although this study establishes a strong theoretical foundation, further empirical research is necessary to validate the proposed conceptual framework. Future studies should examine the model across different regulatory, technological, and cultural contexts to evaluate its practical effectiveness. Particular attention should be given to blockchain scalability solutions, such as layer-two architectures, sharding, and hybrid consensus mechanisms, as well as privacy-preserving techniques like zero-knowledge proofs and off-chain data management. Additionally, governance frameworks related to regulatory harmonization, cross-border compliance, and institutional accountability require deeper investigation. Empirical case studies, pilot implementations, and cross-country comparative analyses would help provide measurable insights into blockchain's role in creating secure, transparent, and sustainable digital payment ecosystems.

7. DECLARATIONS

7.1. About Authors

Ariesya Aprillia (AA) https://orcid.org/0000-0003-0152-2348

Denok Wahyudi Setyo Rahayu (DW) https://orcid.org/0009-0000-6167-6352

Arista Ratih (AR) https://orcid.org/0009-0007-4519-5277

Thomas Green (TG) https://orcid.org/0009-0001-7048-2231

7.2. Author Contributions

Conceptualization: AA, DW, and AR; Methodology: TG; Software: DW; Validation: AA and AR; Formal Analysis: TG and AR; Investigation: DW; Resources: AA; Data Curation: TG; Writing Original Draft Preparation: AR and DW; Writing Review and Editing: TG; Visualization: AA; All authors, AA, DW, AR and TG, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] R. G. Guntara, M. N. Nurfirmansyah *et al.*, "Blockchain implementation in e-commerce to improve the security online transactions," *Journal of Scientific Research, Education, and Technology (JSRET)*, vol. 2, no. 1, pp. 328–338, 2023.

[2] A. K. Sule, N. L. Eyo-Udo, E. C. Onukwulu, M. O. Agho, and C. Azubuike, "Implementing blockchain for secure and efficient cross-border payment systems," *International Journal of Research and Innovation in Applied Science*, vol. 9, no. 12, pp. 508–535, 2024.

[3] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: from anomaly detection to risk management," *Financial Innovation*, vol. 9, no. 1, p. 66, 2023.

[4] N. P. Sable, V. U. Rathod, R. Sable, and G. R. Shinde, "The secure e-wallet powered by blockchain and distributed ledger technology," in *2022 IEEE Pune Section International Conference (PuneCon)*. IEEE, 2022, pp. 1–5.

[5] S.-I. Kim and S.-H. Kim, "E-commerce payment model using blockchain," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1673–1685, 2022.

[6] J. Galang and H. Ramdhan, "Analysis of the acceptance level of e-wallet as a non-cash payment method among indonesian students," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 1, pp. 67–75, 2023.

[7] D. Dinarwati, M. G. Ilham, and F. Rahardja, "Cybersecurity risk assessment framework for blockchain-based financial technology applications," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 168–179, 2025.

[8] A. M. Sahi, H. Khalid, A. F. Abbas, K. Zedan, S. F. Khatib, and H. Al Amosh, "The research trend of security and privacy in digital payment," in *Informatics*, vol. 9, no. 2. MDPI, 2022, p. 32.

[9] M. A. D. Yuda and S. Watini, "Implementation of blockchain technology as the latest solution to improve data security and integrity," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 1, pp. 71–82, 2023.

[10] G. K. Patra, S. K. Rajaram, V. N. Boddapati, C. Kuraku, and H. K. Gollangi, "Advancing digital payment systems: combining ai, big data, and biometric authentication for enhanced security," *International Journal of Engineering and Computer Science*, vol. 11, no. 08, pp. 10–18 535, 2022.

[11] L. Meria, S. Fabian, T. Mariyanti *et al.*, "Digital transformation and blockchain technology: A viewpoint from emerging markets," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 50–57, 2024.

[12] A. A. Nurdin, A. B. Pamungkas, and A. N. Kholifah, "Factors that influence the use of digital payments as ease of transactions in the digital era," *MATRIX: Jurnal Manajemen Teknologi Dan Informatika*, vol. 13, no. 1, pp. 25–32, 2023.

[13] R. A. Kasri, B. S. Indrastomo, N. D. Hendranastiti, and M. B. Prasetyo, "Digital payment and banking stability in emerging economy with dual banking system," *Heliyon*, vol. 8, no. 11, 2022.

[14] M. A. W. Saputra, D. Ochtaffia, D. Apriani, S. C. Yusfi, and M. Gori, "Blockchain applications in education affecting challenges and problems in digital," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 15–23, 2023.

[15] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, "Blockchain technology: Revolutionizing data integrity and security in digital environments," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[16] R. Ly and B. Ly, "Digital payment systems in an emerging economy," *Computers in Human Behavior Reports*, vol. 16, p. 100517, 2024.

[17] A. Rizky, R. W. Nugroho, W. Sejati, O. Sy *et al.*, "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 183–192, 2025.
[18] J. I. Saputro, A. A. Rahmadani, D. M. Sriyono, H. Yuliyanto, and N. A. Silaban, "Human development and the business model impact of bitcoin transactions," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 64–69, 2023.
[19] J. Putrevu and C. Mertzanis, "The adoption of digital payments in emerging economies: challenges and policy responses," *Digital Policy, Regulation and Governance*, vol. 26, no. 5, pp. 476–500, 2024.
[20] R. K. Ray, F. R. Chowdhury, and M. R. Hasan, "Blockchain applications in retail cybersecurity: Enhancing supply chain integrity, secure transactions, and data protection," *Journal of business and management studies*, vol. 6, no. 1, pp. 206–214, 2024.
[21] K. Kajol, R. Singh, and J. Paul, "Adoption of digital financial transactions: A review of literature and future research agenda," *Technological Forecasting and Social Change*, vol. 184, p. 121991, 2022.
[22] M. Rahman, I. Ismail, S. Bahri, and M. K. Rahman, "An empirical analysis of cashless payment systems for business transactions," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 4, p. 213, 2022.
[23] A. Roy and S. Tinny, "Cybersecurity and blockchain for secure financial transactions: Evaluating, implementing, and mitigating risks of digital payments," *INTERNATIONAL JOURNAL OF APPLIED*, vol. 1, no. 2, pp. 38–48, 2023.
[24] A. Rizky, A. Gunawan, M. A. Komara, M. Madani, and E. Harris, "Optimization of machine learning algorithms for fraud detection in e-payment systems," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 55–64, 2025.
[25] N. L. Eyo-Udo, M. O. Agho, E. C. Onukwulu, A. K. Sule, C. Azubuike, L. Nigeria, and P. Nigeria, "Advances in blockchain solutions for secure and efficient cross-border payment systems," *International Journal of Research and Innovation in Applied Science*, vol. 9, no. 12, pp. 536–563, 2024.
[26] M. Gang, "Enhancing global finance: A blockchainbased solution for efficient and cost-effective cross-border payments," *Journal of Trends in Financial and Economics*, vol. 2, no. 2, 2025.
[27] M. Yusup, E. Sukmawati, R. Ramadhan, M. I. Suhaepi, S. Zebua, and N. Amallia, "Blockchain technology for cashless investments and transactions in digital era with swot approach," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 17–23, 2022.
[28] H. Siagian, Z. J. H. Tarigan, S. R. Basana, and R. Basuki, "The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform." *International Journal of Data & Network Science*, vol. 6, no. 3, 2022.
[29] D. Yusuf, R. Anugrah, M. Komara, D. Julianingsih, and E. Garcia, "Leveraging blockchain technology to strengthen cybersecurity in financial transactions: A comprehensive analysis," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 119–125, 2024.
[30] V. Chang, A. Di Stefano, Z. Sun, G. Fortino *et al.*, "Digital payment fraud detection methods in digital ages and industry 4.0," *Computers and Electrical Engineering*, vol. 100, p. 107734, 2022.
[31] A. Sutarman, D. Juliastuti, I. Yati, L. P. Pasha *et al.*, "Enhancing security and privacy in blockchain systems for tax administration," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 145–155, 2025.
[32] N. Ani, S. Millah, and P. A. Sunarya, "Optimizing online business security with blockchain technology," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 67–80, 2024.
[33] S. Azizah, B. K. Bintoro, R. D. Octavyra *et al.*, "Determining factors of continuance intention to use qr code mobile payment on urban millennials in indonesia empirical study on mobile payment funds," *ADI Journal on Recent Innovation*, vol. 3, no. 2, pp. 121–138, 2022.
[34] M. R. I. Bhuiyan, M. S. Akter, and S. Islam, "How does digital payment transform society as a cashless society? an empirical study in the developing economy," *Journal of Science and Technology Policy Management*, vol. 16, no. 4, pp. 756–774, 2025.
[35] T. Handra, S. Purnama, A. J. Kusumo, and D. Bennet, "Blockchain in digital transformation: Enhancing security, transparency, and efficiency in modern systems," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 23–28, 2024.
[36] M. N. Seldal and E. K. Nyhus, "Financial vulnerability, financial literacy, and the use of digital payment technologies," *Journal of Consumer Policy*, vol. 45, no. 2, pp. 281–306, 2022.
[37] L. Sanbella, I. Van Versie, and S. Audiah, "Online marketing strategy optimization to increase sales and

e-commerce development: An integrated approach in the digital age," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 54–66, 2024.
[38] U. Rahardja, I. D. Hapsari, P. H. Putra, and A. N. Hidayanto, "Technological readiness and its impact on mobile payment usage: A case study of go-pay," *Cogent Engineering*, vol. 10, no. 1, p. 2171566, 2023.
[39] D. Bennet, L. Maria, Y. P. A. Sanjaya, and A. R. A. Zahra, "Blockchain technology: Revolutionizing transactions in the digital age," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 192–199, 2024.
[40] Z. Hatefi, M. Bayat, M. R. Alaghband, N. Hamian, and S. M. Pournaghi, "A conditional privacy-preserving fair electronic payment scheme based on blockchain without trusted third party," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 8, pp. 10 089–10 102, 2023.
[41] T. Norbu, J. Y. Park, K. W. Wong, and H. Cui, "Factors affecting trust and acceptance for blockchain adoption in digital payment systems: A systematic review," *Future Internet*, vol. 16, no. 3, p. 106, 2024.
[42] B. Rawat and D. Maulidditya, "Entrepreneurship in information technology as a method for improving student creativity in the digital economy," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 1, pp. 32–37, 2022.
[43] A. Pamisetty, H. K. Sriram, M. Malempati, S. R. Challa, and S. Mashetty, "Ai-driven optimization of intelligent supply chains and payment systems: Enhancing security, tax compliance, and audit efficiency in financial operations," *Tax Compliance, and Audit Efficiency in Financial Operations (December 15, 2022)*, 2022.
[44] G. A. Pangilinan, A. Tambunan, and E. D. Astuti, "Tokopedia e-commerce is being used to present opportunities for young business owners to succeed in the digital economy amid the pandemic," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 182–191, 2023.
[45] L. N. Nasution, D. M. Rangkuty, and S. M. Putra, "The digital payment system: How does it impact indonesia's poverty?" *ABAC Journal*, vol. 44, no. 3, p. 228, 2024.
[46] J. Williams, A. G. Prawiyogi, M. Rodriguez, and I. Kovac, "Enhancing circular economy with digital technologies: A pls-sem approach," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 140–151, 2024.
[47] F. Wang, N. Yang, P. M. Shakeel, and V. Saravanan, "Machine learning for mobile network payment security evaluation system," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4226, 2024.
[48] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
[49] D. Mohanty, D. Anand, H. M. Aljahdali, and S. G. Villar, "Blockchain interoperability: Towards a sustainable payment system," *Sustainability*, vol. 14, no. 2, p. 913, 2022.
[50] P. Rani, R. K. Sachan, and S. Kukreja, "Academic payment tokenization: an online payment system for academia utilizing non-fungible tokens and permissionless blockchain," *Procedia Computer Science*, vol. 230, pp. 347–356, 2023.
[51] Y. Xiao, C. Zhou, X. Guo, Y. Song, and C. Chen, "A novel decentralized e-commerce transaction system based on blockchain," *Applied Sciences*, vol. 12, no. 12, p. 5770, 2022.
[52] J. A. Jafri, S. I. M. Amin, A. A. Rahman, and S. M. Nor, "A systematic literature review of the role of trust and security on fintech adoption in banking," *Heliyon*, vol. 10, no. 1, 2024.
[53] T. Gross, T. J. Layton, and D. Prinz, "The liquidity sensitivity of healthcare consumption: Evidence from social security payments," *American Economic Review: Insights*, vol. 4, no. 2, pp. 175–190, 2022.
[54] R. Toorajipour, P. Oghazi, V. Sohrabpour, P. C. Patel, and R. Mostaghel, "Block by block: A blockchain-based peer-to-peer business transaction for international trade," *Technological Forecasting and Social Change*, vol. 180, p. 121714, 2022.
[55] L. Zhao, J. Zhang, and L. Zhong, "A blockchain-based transaction system with payment statistics and supervision," *Connection Science*, vol. 34, no. 1, pp. 1751–1771, 2022.