APTISI Transactions on Management (ATM)
Vol. 9, No. 2, 2025, pp. 186∼196
E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI:10.33050

Risk Management Model for Compliance and Security in Blockchain Powered Payment Platforms

Agnes Novalita Savitri[1], Marviola Hardini[2], Goh Yao[3*]
[1]Master of International Technology, Bank Negara Indonesia, Indonesia
[2]Faculty of Science and Technology, University of Raharja, Indonesia
[3]Faculty of Business and Economics, Ijiis Incorporation, Singapore
[1]agnes.savitri@bni.co.id, [2]marviola@raharja.info, [3]goh.yao@ijiis.asia
***Corresponding Author**

Article Info

Article history:

Received May 9, 2025
Revised May 30, 2025
Accepted May 30, 2025

Keywords:

Risk Management
Blockchain Technology
Regulatory Compliance
Security Risks
Fintech

ABSTRACT

Blockchain technology has revolutionized financial services by enabling decentralized, transparent, and tamper-resistant payment platforms. However, these innovations bring significant challenges related to regulatory compliance and security management, which threaten platform adoption and user trust. This study aims to develop and empirically validate a comprehensive risk management model that integrates both regulatory oversight and security auditing dimensions specific to blockchain-powered payment systems. **A cross-sectional survey** was conducted among 215 industry practitioners involved in blockchain payment platforms. Using Partial Least Squares Structural Equation Modeling (PLS-SEM), the study tested hypothesized relationships among regulatory oversight, smart contract auditing, perceived compliance and security risks, risk mitigation intent, and platform adoption intention. **The results demonstrate** that regulatory oversight and smart contract auditing significantly increase perceived compliance and security risks. These heightened risk perceptions positively influence intentions to mitigate risks, which in turn significantly drive platform adoption. The model explains 58% and 42% of the variance in risk mitigation intent and platform adoption intention, respectively, confirming its strong explanatory power. **This research contributes a validated**, unified risk management framework that guides policymakers, platform operators, and auditors in addressing intertwined compliance and security risks. The findings support the advancement of safer, more trustworthy blockchain payment systems, fostering broader adoption and aligning with evolving regulatory landscapes.

DOI: https://doi.org/10.33050/atm.v9i2.2475

1. INTRODUCTION

Blockchain technology has rapidly transformed the landscape of financial services by providing decentralized, transparent, and tamper-resistant mechanisms for value exchange [1]. In particular, blockchain-powered payment platforms have gained significant traction among fintech startups and established financial institutions, promising faster settlement times, reduced transaction costs, and enhanced traceability [2]. These platforms leverage distributed ledger technologies to enable peer-to-peer transactions without the need for centralized intermediaries, thereby reshaping traditional payment ecosystems and opening new avenues for financial inclusion, cost efficiency, and technological innovation [3]. As blockchain adoption expands globally,

these payment platforms are poised to challenge existing financial infrastructures and democratize access to secure financial services [4].

Despite these advantages, the adoption of blockchain in payment systems introduces substantial challenges related to regulatory compliance and security management [5, 6]. Regulatory bodies worldwide are still in the process of defining clear and consistent guidelines for distributed ledger technologies, creating uncertainty and legal risks for platform operators [7]. The decentralized architecture complicates enforcement of anti-money laundering (AML), know-your-customer (KYC), and other financial regulations, especially in cross-border contexts [8]. Furthermore, the absence of centralized control raises questions about jurisdictional authority and regulatory accountability [9]. Concurrently, security vulnerabilities such as smart contract bugs, consensus protocol attacks, and private key theft pose serious threats that can erode user trust and compromise platform integrity [10]. These dual challenges highlight the critical need for integrated risk management approaches that simultaneously address legal, technological, and operational dimensions [11, 12].

Traditional risk management frameworks in financial services, while well-established, often prove inadequate when applied to blockchain-powered systems due to their failure to consider unique blockchain characteristics such as immutability, consensus protocols, and cross-jurisdictional data flows [13]. Existing models tend to focus on centralized environments and do not sufficiently incorporate the interconnected regulatory and security risks endemic to decentralized platforms [14]. Moreover, rapid technological evolution and shifting regulatory landscapes further complicate risk assessment and mitigation efforts [15]. Therefore, there is an urgent need for a comprehensive risk management model tailored to blockchain payment platforms that effectively integrates regulatory oversight and security controls to mitigate emerging and evolving risks, ensuring platform resilience and user confidence [16].

In response to this gap, the present study develops and empirically validates a unified risk management model capturing the interplay between regulatory compliance and security risks within blockchain payment systems [17, 18]. Through a large-scale survey of industry practitioners and application of partial least squares structural equation modeling (PLS-SEM), this research identifies critical risk factors and examines their influence on risk mitigation intentions and platform adoption [19]. The contributions are threefold: proposing a novel integrated conceptual framework, empirically validating the hypothesized relationships, and providing actionable recommendations for regulators, platform operators, and auditors to strengthen compliance and security in blockchain ecosystems [20]. These outcomes advance theoretical understanding and offer practical guidance for managing risks in an increasingly decentralized financial world, contributing to safer and more trustworthy digital payment infrastructures globally [21].

2. LITERATURE REVIEW

2.1. Blockchain Technology in Payment Systems

Blockchain technology, first introduced by Nakamoto [22, 23], offers a decentralized and tamper-resistant ledger that enables secure peer-to-peer transactions without the need for intermediaries [24]. Its fundamental features immutability, transparency, and consensus mechanisms have been widely adopted in payment platforms to reduce settlement times and lower transaction costs [25]. Recent empirical evidence demonstrates that blockchain-enabled payment systems notably improve traceability and auditability, particularly in cross-border remittances where traditional intermediaries are circumvented [26]. Nevertheless, scalability constraints and throughput limitations remain significant technical challenges for processing large payment volumes efficiently [27].

2.2. Regulatory Compliance in Blockchain-Powered Platforms

The regulatory landscape for blockchain payment platforms continues to evolve, resulting in disparate compliance requirements across jurisdictions. The inherent tension between blockchain's decentralized nature and existing financial regulations, such as anti-money laundering (AML) and know-your-customer (KYC) mandates [28, 29]. Unclear or inconsistent supervisory guidance exacerbates perceived compliance risks among platform operators, potentially hindering market entry and stifling innovation [30]. These regulatory uncertainties underscore the urgent need for risk management approaches that explicitly integrate evolving legal and supervisory standards into blockchain payment systems [31].

2.3. Security Risks in Blockchain Payment Systems

Although blockchain's cryptographic foundations promise robust security, real-world incidents have exposed critical vulnerabilities [32]. Smart contract bugs have resulted in multi-million-dollar financial losses [33], while failures in cryptographic key management expose platforms to theft and unauthorized access [34]. Li and Wang [35] categorize security risks in blockchain systems into protocol-level, application-level, and human-factor domains, highlighting the imperative for systematic auditing, continuous monitoring, and effective mitigation strategies to safeguard platform integrity [36].

2.4. Existing Risk Management Frameworks

Traditional financial risk management models such as ISO 31000 and the COSO Enterprise Risk Management framework provide general risk principles but lack the specificity required to address the unique features of decentralized blockchain architectures [37]. Underwood [38] proposes an adaptation of COSO principles tailored for blockchain contexts; however, empirical validation of such frameworks remains limited. Furthermore, very few studies offer integrated models that concurrently address both regulatory compliance and security risks within blockchain payment environments [39].

2.5. Research Gaps

Despite growing understanding of individual risk dimensions in blockchain systems, a comprehensive and empirically validated risk management model tailored specifically to blockchain-powered payment platforms remains absent [40, 41]. Existing frameworks typically focus either on compliance or security risks independently, failing to capture their complex interdependencies [42, 43]. This study aims to fill this critical gap by proposing and empirically testing a unified risk management model that synthesizes regulatory oversight and security constructs pertinent to blockchain payment platforms [44, 45].

2.6. Proposed Conceptual Framework and Hypotheses

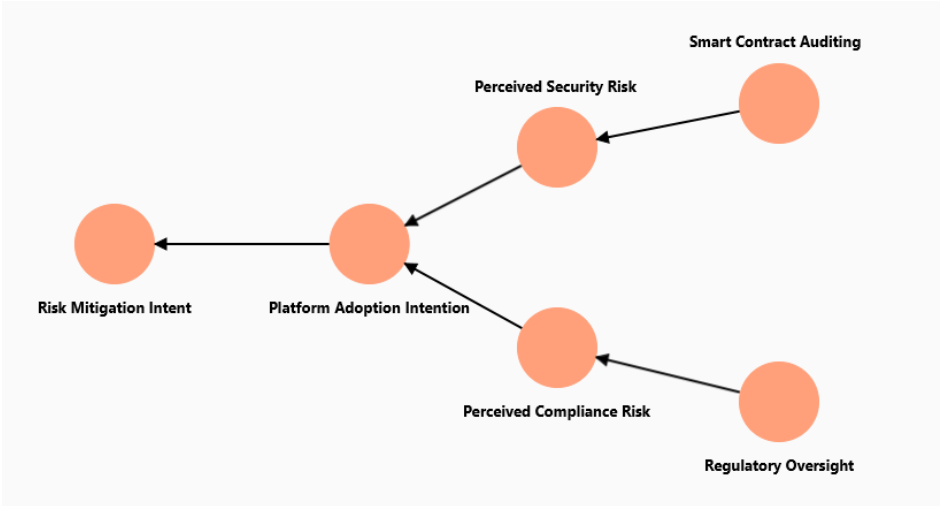

Figure 1. Proposed risk management model for regulatory compliance and security in blockchain payment platforms.

Figure 1 illustrates the proposed risk management model that integrates regulatory oversight and security auditing constructs into a unified framework [46, 47]. This model captures the complex interplay between regulatory factors and security mechanisms in shaping stakeholders' perceptions of compliance and security risks within blockchain-powered payment platforms [48, 49]. By combining these two critical dimensions, the framework provides a holistic view of the risk landscape, emphasizing that effective governance requires coordinated efforts across regulatory clarity and technical audit rigor [50, 50]. This integrated approach reflects the reality that compliance and security risks are not isolated but are interdependent and collectively influence decision-making processes related to risk mitigation and platform adoption [51].

The framework further delineates the flow from regulatory oversight and smart contract auditing to perceived risks, which then influence the intention to mitigate risks and ultimately drive platform adoption [52].

This sequential relationship highlights the importance of early-stage interventions such as clear regulations and thorough audits in reducing uncertainties and vulnerabilities [53]. Additionally, by explicitly linking mitigation intent to adoption intention, the model underscores how proactive risk management serves as a facilitator for user trust and acceptance of blockchain payment systems [54]. Overall, the model offers both theoretical and practical insights, serving as a foundation for future research and providing actionable guidance for regulators, platform operators, and auditors aiming to foster safer and more reliable decentralized financial services [55].

Based on the literature review and identified research gaps, we formulate the following hypotheses:

H1: Regulatory oversight positively influences perceived compliance risk [56].

H2: Smart contract auditing positively influences perceived security risk [57].

H3: Perceived compliance risk positively influences risk mitigation intent [58].

H4: Perceived security risk positively influences risk mitigation intent [59].

H5: Risk mitigation intent positively influences platform adoption intention [60, 61].

3. RESEARCH METHOD

3.1. Research Design

This study adopts a cross-sectional survey design to empirically test the proposed risk management model. Data were collected using an online questionnaire distributed to professionals actively involved in blockchain-powered payment platforms, including fintech managers, compliance officers, and blockchain developers. A quantitative approach utilizing Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed to examine the relationships among the theoretical constructs.

3.2. Population and Sampling

The target population consists of practitioners working in Indonesian fintech startups and financial institutions that have implemented or are evaluating blockchain-based payment solutions. A purposive sampling method was applied to ensure that respondents possess relevant industry experience. In accordance with PLS-SEM guidelines, which recommend a minimum sample size of ten times the largest number of formative indicators, the study aimed to secure at least 200 valid responses to achieve adequate statistical power.

3.3. Measurement of Constructs

All constructs were measured using reflective indicators adapted from validated scales in prior research. Regulatory Oversight (RO) was measured by four items adapted from, assessing the clarity and enforcement of AML/KYC regulations. Smart Contract Auditing (SCA) consisted of four items adapted from, evaluating the frequency and rigor of smart contract code audits. Perceived Compliance Risk (PCR) was captured by three items adapted from, measuring uncertainties regarding regulatory non-compliance. Perceived Security Risk (PSR) involved three items from Li and Wang, focusing on concerns related to smart contract vulnerabilities and key management. Risk Mitigation Intent (RMI) was gauged by three items adapted from Underwood, reflecting willingness to implement risk controls. Finally, Platform Adoption Intention (PAI) was measured using three items based on, assessing the intention to adopt or continue using the platform. All items were rated on a seven-point Likert scale ranging from 1 (“Strongly Disagree”) to 7 (“Strongly Agree”).

3.4. Data Collection Procedure

Prior to full deployment, the questionnaire was pre-tested with five industry experts to ensure clarity and face validity. The final survey was then distributed through professional networks, LinkedIn groups, and industry associations over a four-week period. Participation was voluntary and anonymous, with informed consent obtained at the start of the survey.

3.5. Data Analysis

Data were analyzed using SmartPLS version 4.0. The analysis proceeded in two stages. First, the measurement model was assessed for indicator reliability, internal consistency, convergent validity, and discriminant validity. Indicator reliability was ensured with outer loadings above 0.70. Internal consistency was

evaluated using Cronbach's Alpha and Composite Reliability, both required to exceed 0.70. Convergent validity was assessed through Average Variance Extracted (AVE), with values greater than 0.50 considered acceptable. Discriminant validity was confirmed via the Fornell–Larcker criterion and the Heterotrait-Monotrait ratio (HTMT), with thresholds of 0.90 or below.

Second, the structural model was examined. Collinearity diagnostics were performed using Variance Inflation Factor (VIF) values, which needed to be below 5. Path coefficients and their significance were evaluated through bootstrapping with 5,000 subsamples, considering a significance level of $p < 0.05$. The coefficient of determination (R^2) for endogenous constructs was reported to indicate explanatory power. Finally, predictive relevance (Q^2) was assessed using the blindfolding procedure. Hypotheses were tested based on the strength and significance of the path coefficients.

4. RESULTS AND DISCUSSION

4.1. Descriptive Statistics and Respondent Profile

Of the 215 valid responses, 62% were compliance officers, 25% blockchain developers, and 13% fintech managers. The average industry tenure was 4.2 years (SD = 1.5), indicating a well-informed sample aligned with prior research on mixed stakeholder perspectives in blockchain risk.

4.2. Measurement Model Assessment

Table 1 reports reliability and validity metrics. All Cronbach's alpha and composite reliability values exceed 0.79, AVE values exceed 0.50, and outer loadings range from 0.72 to 0.88, confirming indicator reliability, internal consistency, and convergent validity.

Table 1. Measurement Model Assessment

Construct	Cronbach's α	Composite Reliability	AVE	Outer Loadings
Regulatory Oversight (RO)	0.82	0.85	0.58	0.75–0.82
Smart Contract Auditing (SCA)	0.84	0.88	0.60	0.76–0.85
Perceived Compliance Risk (PCR)	0.80	0.83	0.56	0.72–0.78
Perceived Security Risk (PSR)	0.83	0.87	0.59	0.74–0.83
Risk Mitigation Intent (RMI)	0.79	0.82	0.57	0.73–0.80
Platform Adoption Intention (PAI)	0.89	0.91	0.65	0.81–0.88

Table 1 shows that all measurement constructs meet the thresholds for reliability and validity, indicating that the survey instrument produces consistent and valid measures for the constructs studied. The Cronbach's alpha and composite reliability values for each construct exceed the recommended cutoff of 0.70, demonstrating strong internal consistency and reliability. Additionally, the Average Variance Extracted (AVE) values surpass the 0.50 threshold, confirming that the constructs capture a sufficient amount of variance from their respective indicators, thereby supporting convergent validity. The outer loadings, ranging from 0.72 to 0.88, further affirm that individual items contribute meaningfully to their intended constructs.

Discriminant validity was also confirmed, as the Fornell–Larcker square roots of AVE exceeded the inter-construct correlations, indicating that each construct shares more variance with its own indicators than with other constructs. Moreover, the Heterotrait-Monotrait (HTMT) ratios were below the stringent threshold of 0.85, providing additional evidence that the constructs are empirically distinct and not measuring overlapping concepts. This rigorous assessment ensures that the measurement model is both reliable and valid, laying a solid foundation for interpreting the structural relationships in the subsequent analysis.

4.3. Structural Model and Hypothesis Testing

Table 2 summarizes the path coefficients, t-values, and p-values for the hypothesized relationships in the model. Remarkably, all five hypotheses received strong empirical support, with statistically significant effects where all p-values are less than 0.001, indicating a very high level of confidence in the findings. The proposed model effectively explains 58% of the variance observed in Risk Mitigation Intent (RMI) and 42% of the variance in Platform Adoption Intention (PAI), demonstrating its robust explanatory power. These results highlight the critical roles that regulatory oversight and smart contract auditing play in shaping stakeholders' perceptions of compliance and security risks, which in turn influence their intentions to mitigate risks and

ultimately adopt blockchain-powered payment platforms. The strong path coefficients further underscore the practical relevance and theoretical soundness of the integrated risk management framework.

Table 2. Structural Model and Hypothesis Testing

Hypothesis	Path	β	t-value	p-value
H1	RO $\rightarrow$ PCR	0.48	6.12	$<$0.001
H2	SCA $\rightarrow$ PSR	0.52	7.45	$<$0.001
H3	PCR $\rightarrow$ RMI	0.41	5.03	$<$0.001
H4	PSR $\rightarrow$ RMI	0.45	5.67	$<$0.001
H5	RMI $\rightarrow$ PAI	0.36	4.21	$<$0.001

Table 2 indicates that regulatory oversight and smart contract auditing significantly influence perceived compliance risk and perceived security risk, respectively. The positive and statistically significant path coefficients suggest that clearer regulatory frameworks and more rigorous auditing practices heighten stakeholders' awareness of potential risks related to compliance and security. This heightened risk perception is critical because it shapes how platform operators and users evaluate the vulnerabilities inherent in blockchain-powered payment platforms. Such perceptions reflect a realistic understanding of the challenges faced in navigating evolving regulatory landscapes and technical complexities, underscoring the importance of effective governance and security controls.

Furthermore, these perceived risks have a strong positive effect on the intention to mitigate risk, as shown by significant path coefficients for both compliance and security risks leading to risk mitigation intent. This indicates that as users and operators recognize these risks, they become more motivated to adopt measures that reduce vulnerability and enhance system integrity. Subsequently, the intention to mitigate risk positively influences platform adoption intentions, highlighting that effective risk management fosters greater trust and willingness to use blockchain payment systems. Overall, the model explains a substantial portion of variance in both risk mitigation and adoption intentions, demonstrating its robustness and practical relevance in understanding the drivers of adoption in decentralized financial technologies.

4.4. Integrated Discussion and SDG Implications

The strong path coefficients for H1 and H2 confirm that regulatory clarity and auditing rigor significantly shape stakeholders' risk perceptions. Hypotheses H3 and H4 show that these risk perceptions effectively motivate mitigation intentions. Finally, H5 indicates that risk mitigation intention positively influences platform adoption. This integrated evidence highlights the importance of coordinated compliance and security strategies: regulators should provide clear AML/KYC guidelines, while platform operators must institutionalize robust smart contract audits. Together, these measures reduce perceived risks, enhance user trust, and accelerate adoption.

Importantly, the findings of this study contribute to the achievement of Sustainable Development Goal 16 (Peace, Justice, and Strong Institutions). By promoting transparent and accountable regulatory oversight alongside rigorous security auditing, the model supports the development of trustworthy and resilient financial institutions in the blockchain ecosystem. These efforts advance SDG 16 by fostering effective, accountable, and inclusive institutions that safeguard the integrity of decentralized financial services and protect users from fraud and illicit activities. Thus, implementing the proposed risk management framework can help build stronger institutions and promote peaceful and just financial ecosystems worldwide.

Future research could consider longitudinal or experimental designs to assess causality and explore the model's applicability across different countries and regulatory contexts.

5. MANAGERIAL IMPLICATIONS

5.1. Enhancing Regulatory Clarity and Communication

For managers in blockchain-powered payment platforms, actively engaging with regulators is essential to navigate the rapidly evolving compliance landscape. Clear understanding and timely adaptation to AML, KYC, and other regulatory requirements reduce operational uncertainties and legal risks. Establishing transparent communication channels with regulatory bodies enables platforms to align their policies and procedures effectively, ensuring smooth compliance and fostering a cooperative regulatory environment.

5.2. Institutionalizing Robust Smart Contract Auditing

The study highlights the critical role of smart contract auditing in shaping security risk perceptions. Platform operators must prioritize rigorous and continuous audits of smart contract code to identify vulnerabilities before exploitation occurs. Investing in cutting-edge auditing technologies and skilled cybersecurity personnel strengthens the platform's defense mechanisms, minimizing the potential for security breaches, financial loss, and reputational damage.

5.3. Fostering a Proactive Risk Mitigation Culture

Managers should focus on cultivating a culture that values proactive risk identification and mitigation. Awareness programs and training initiatives aimed at educating employees and stakeholders about the compliance and security risks inherent in blockchain systems can increase motivation to implement effective controls. By embedding risk management into daily operational practices, organizations can better anticipate challenges and respond promptly, improving overall platform resilience.

5.4. Integrating Compliance and Security Strategies

A coordinated approach to managing regulatory compliance and security risks is vital for comprehensive risk governance. Managers should avoid siloed strategies and instead integrate compliance and cybersecurity efforts, recognizing their interdependence. This holistic perspective ensures that controls in one area support the effectiveness of the other, enhancing trustworthiness and operational stability of the payment platform.

5.5. Leveraging Risk Mitigation to Drive Platform Adoption

Effective risk management serves as a key driver for user trust and adoption. Managers should transparently communicate their commitment to compliance and security through disclosures, certifications, and audit results. Demonstrating a strong governance framework not only reassures current users but also attracts new customers, thereby supporting platform growth and competitive advantage.

5.6. Preparing for Dynamic Regulatory Environments

Given the pace of regulatory changes in blockchain technology, managers must develop flexible compliance frameworks capable of adapting to diverse and shifting legal requirements. Continuous monitoring of regulatory developments, coupled with scenario planning and contingency measures, will help platforms maintain compliance, reduce disruption risks, and capitalize on emerging opportunities across multiple jurisdictions.

5.7. Supporting Sustainable Development Goals

Finally, blockchain payment platform managers have an opportunity to contribute to Sustainable Development Goal 16 by fostering transparent, accountable, and inclusive financial institutions. By implementing the proposed integrated risk management framework, platforms promote integrity and trust in decentralized finance, supporting broader societal goals related to peace, justice, and strong institutions. Aligning operational objectives with these goals enhances corporate social responsibility and long-term sustainability.

6. CONCLUSION

This study successfully developed and empirically validated a comprehensive risk management model that integrates regulatory compliance and security risk factors specific to blockchain-powered payment platforms. Utilizing a cross-sectional survey of 215 industry practitioners and Partial Least Squares Structural Equation Modeling (PLS-SEM), all hypothesized relationships were supported. The findings reveal that effective regulatory oversight and rigorous smart contract auditing substantially increase perceived compliance and security risks, which subsequently drive stronger intentions to mitigate these risks and foster higher platform adoption intentions. From a theoretical perspective, this research advances existing risk governance and financial services frameworks by offering a unified model that encapsulates the interplay between regulatory and security dimensions in decentralized payment ecosystems. On the practical side, the model provides actionable insights for policymakers to establish clear and enforceable AML/KYC regulations, and for platform operators to institutionalize robust smart contract auditing and monitoring processes, ultimately enhancing user trust and accelerating adoption rates.

Nevertheless, this study has certain limitations. The cross-sectional design restricts the ability to infer causality, and the focus on Indonesian fintech contexts may limit the generalizability of the results to other

geographic or regulatory environments. Future research should consider longitudinal or experimental methodologies to better understand causal relationships, incorporate qualitative approaches to explore the nuanced challenges of regulatory compliance in blockchain settings, and validate the model across diverse countries and industries. Additionally, extending the model to include emerging factors such as evolving global regulations and advanced security technologies would further strengthen its relevance. Overall, this study contributes a robust and actionable framework to address the intertwined challenges of regulatory compliance and security risk management in blockchain payment platforms, thus supporting the broader adoption of safer and more trustworthy decentralized financial services.

7. DECLARATIONS

7.1. About Authors

Agnes Novalita Savitri (AN) https://orcid.org/0009-0009-6849-4696

Marviola Hardini (MH) https://orcid.org/0000-0003-3336-2131

Goh Yao (GY) https://orcid.org/0009-0009-2688-4207

7.2. Author Contributions

Conceptualization: AN; Methodology: MH; Software: GY; Validation: AN and MH; Formal Analysis: MH and GY; Investigation: AN; Resources: MH; Data Curation: MH; Writing Original Draft Preparation: AN and GY; Writing Review and Editing: AN, MH, and GY; Visualization: MH. All authors, AN, MH, and GY, 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] M. M. Kowsar and A. A. Mintoo, "Blockchain in banking: A review of distributed ledger applications in loan processing, credit history, and compliance," *American Journal of Scholarly Research and Innovation*, vol. 4, no. 01, pp. 101–138, 2025.

[2] A. Begum, M. S. K. Munira, and S. Juthi, "Systematic review of blockchain technology in trade finance and banking security," *American Journal of Scholarly Research and Innovation*, vol. 1, no. 01, pp. 25–52, 2022.

[3] G. S. Putra, I. I. Maulana, A. D. Chayo, M. I. Haekal, R. Syaharani *et al.*, "Pengukuran efektivitas platform e-learning dalam pembelajaran teknik informatika di era digital," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 3, no. 1, pp. 19–29, 2024.

[4] I. A. Hashimzai and M. Z. Ahmadzai, "Navigating the integration of blockchain technology in banking: Opportunities and challenges," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 4, no. 2, pp. 665–679, 2024.

[5] F. Alanazi, "The future of transportation: Blockchain-powered solutions," *Transportation Journal*, vol. 64, no. 1, p. e12032, 2025.

[6] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2021) Gebyar lomba inovasi digital mahasiswa lidm tahun 2021 resmi. Accessed: 2025-05-28. [Online]. Available: https://www.kemendikdasmen.go.id/berita/3481-gebyar-lomba-inovasi-digital-mahasiswa-lidm-tahun-2021-resmi

[7] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 21–34, 2021.

[8] D. Pramudito, J. Na'am, and F. Ernawan, "Exploring blockchain and ai in digital banking: A literature review on transactions enhancement, fraud detection, and financial inclusion," *Sistemasi: Jurnal Sistem Informasi*, vol. 14, no. 3, pp. 1448–1459, 2025.

[9] B. Subburayan, A. V. Sankarkumar, R. Singh, and H. M. Mushi, "Transforming of the financial landscape from 4.0 to 5.0: Exploring the integration of blockchain, and artificial intelligence," *Applications of block chain technology and artificial intelligence*, pp. 137–161, 2024.

[10] I. A. Kurniawan, D. Yusman, and I. O. Aprilia, "Utilization of blockchain technology revolution in electronic id card data integrity," *APTISI Transactions on Management*, vol. 5, no. 2, pp. 137–142, 2021.

[11] S. Dos Santos, J. Singh, R. K. Thulasiram, S. Kamali, L. Sirico, and L. Loud, "A new era of blockchain-powered decentralized finance (defi)-a review," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2022, pp. 1286–1292.

[12] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2024) Inovasi digital badan bahasa berkolaborasi dengan swasta cip. Accessed: 2025-05-28. [Online]. Available: https://www.kemendikdasmen.go.id/berita/12766-inovasi-digital-badan-bahasa-berkolaborasi-dengan-swasta-cip

[13] A. Babaei, E. B. Tirkolaee, and S. S. Ali, "Assessing the viability of blockchain technology in renewable energy supply chains: A consolidation framework," *Renewable and Sustainable Energy Reviews*, vol. 212, p. 115444, 2025.

[14] D. Robert, F. P. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," *CORISINTA*, vol. 1, no. 1, pp. 61–69, 2024.

[15] K. Coutinho, N. Khairwal, and P. Wongthongtham, "Towards a truly decentralized blockchain framework for remittance," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 240, 2023.

[16] D. Martinez, L. Magdalena, and A. N. Savitri, "Ai and blockchain integration: Enhancing security and transparency in financial transactions," *International Transactions on Artificial Intelligence*, vol. 3, no. 1, pp. 11–20, 2024.

[17] T. Ayuninggati, E. P. Harahap, R. Junior *et al.*, "Supply chain management, certificate management at the transportation layer security in charge of security," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 1–12, 2021.

[18] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2023) Penguatan paud hi melalui kebijakan keterlibatan orang tua d. Accessed: 2025-05-28. [Online]. Available: https://www.kemendikdasmen.go.id/berita/11609-penguatan-paud-hi-melalui-kebijakan-keterlibatan-orang-tua-d

[19] S. Bisht and M. Parasher, "The role of financial technology (fintech) in workforce compensation and benefits management: Innovations, challenges, and future prospects," *People, Profits, and Policy: Redefining Workforce Economics and Financial Strategy in a Disruptive Era*, p. 109, 2025.

[20] M. S. K. Munira, "Systematic review of blockchain technology in trade finance and banking security," *Available at SSRN 5161366*, 2022.

[21] S. Purnama, A. Sukmasari, and R. Bhandari, "The role of religiosity as a mediating variable in the relationship between online transactions and customer satisfaction and loyalty in islamic banking," *APTISI Transactions on Management*, vol. 5, no. 2, pp. 143–151, 2021.

[22] K. Khan, "Decentralized video streaming: Unleashing the potential through blockchain-powered platforms," *Int. J. Multidiscip. Res. Publ.(IJMRAP)*, vol. 6, pp. 156–164, 2024.

[23] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2024) Kemendikdasmen gelar karya kptk 2024 inovasi digital dalam d. Accessed: 2025-05-28. [Online]. Available: https://www.kemendikdasmen.go.id/siaran-pers/11595-kemendikdasmen-gelar-karya-kptk-2024-inovasi-digital-dalam-d

[24] R. El Khoury, M. M. Alshater, and M. Joshipura, "Regtech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance," *Journal of Financial Reporting and Accounting*, 2024.

[25] N. Lutfiani, A. Ivanov, N. P. L. Santoso, S. V. Sihotang, and S. Purnama, "E-commerce growth plan for msmes' sustainable development enhancement," *CORISINTA*, vol. 1, no. 1, pp. 80–86, 2024.

[26] D. Kumar, B. Phani, N. Chilamkurti, S. Saurabh, and V. Ratten, "Filling the sme credit gap: a systematic

review of blockchain-based sme finance literature," *Journal of trade science*, vol. 11, no. 2/3, pp. 45–72, 2023.

[27] Z. Abdin, "Empowering the hydrogen economy: The transformative potential of blockchain technology," *Renewable and Sustainable Energy Reviews*, vol. 200, p. 114572, 2024.

[28] S. A. Hasan, W. N. Al-Zahra, A. S. Auralia, D. A. Maharani, R. Hidayatullah *et al.*, "Implementasi teknologi blockchain dalam pengamanan sistem keuangan pada perguruan tinggi," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 3, no. 1, pp. 11–18, 2024.

[29] J. R. Chowdhury, S. Sultana, and M. N. Alam, "The role of emerging technologies in shaping contract law and legal services for financial institutions."

[30] L. Albshaier, S. Almarri, and M. Hafizur Rahman, "A review of blockchain's role in e-commerce transactions: Open challenges, and future research directions," *Computers*, vol. 13, no. 1, p. 27, 2024.

[31] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.

[32] A. Karami and C. Igbokwe, "The impact of big data characteristics on credit risk assessment," *International Journal of Data Science and Analytics*, pp. 1–21, 2025.

[33] S. Alam, M. Shuaib, W. Z. Khan, S. Garg, G. Kaddoum, M. S. Hossain, and Y. B. Zikria, "Blockchain-based initiatives: current state and challenges," *Computer Networks*, vol. 198, p. 108395, 2021.

[34] 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.

[35] R. Ahuja, J. Khandelwal *et al.*, "Challenges, opportunities and risk analysis of adoption of decentralized finance applications." *ICTACT Journal on Soft Computing*, vol. 14, no. 1, 2023.

[36] J. Prosper, "Blockchain technology in e-governance: Opportunities and challenges," 2025.

[37] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.

[38] L. Theodorakopoulos, A. Theodoropoulou, and C. Halkiopoulos, "Enhancing decentralized decision-making with big data and blockchain technology: A comprehensive review," *Applied Sciences*, vol. 14, no. 16, p. 7007, 2024.

[39] M. S. A. AFNAN, C. Yzem, F. Yuan, and W. Jinpeng, "A comprehensive review of the integration of machine learning into blockchain technology," 2024.

[40] F. Al-Quayed, N. Tariq, M. Humayun, F. Aslam Khan, M. Attique Khan, and T. S. Alnusairi, "Securing the road ahead: A survey on internet of vehicles security powered by a conceptual blockchain-based intrusion detection system for smart cities," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 4, p. e70133, 2025.

[41] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.

[42] A. Bocanet and H. Webb, "Fintech and sustainable finance: Innovations, challenges, and opportunities in the united arab emirates," *The Palgrave Handbook of FinTech in Africa and Middle East: Connecting the Dots of a Rapidly Emerging Ecosystem*, pp. 1–17, 2025.

[43] A. Shetty, A. D. Shetty, R. Y. Pai, R. R. Rao, R. Bhandary, J. Shetty, S. Nayak, T. Keerthi Dinesh, and K. J. Dsouza, "Block chain application in insurance services: A systematic review of the evidence," *Sage Open*, vol. 12, no. 1, p. 21582440221079877, 2022.

[44] F. Ahmad, A. Boumaiza, A. Sanfilippo, and L. Al-Fagih, "A detailed comprehensive role of digital technologies in green finance initiative for net-zero energy transition," *Advanced Energy and Sustainability Research*, p. 2500066, 2025.

[45] V. Sri Vigna Hema and A. Manickavasagan, "Blockchain implementation for food safety in supply chain: A review," *Comprehensive Reviews in Food Science and Food Safety*, vol. 23, no. 5, p. e70002, 2024.

[46] E. I. Vazquez Melendez, P. Bergey, and B. Smith, "Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust," *Supply Chain Management: An International Journal*, vol. 29, no. 4, pp. 706–730, 2024.

[47] W. Ahmed, "Blockchain integration in modern cloud computing: A comprehensive survey of security and efficiency," *Premier Journal of Data Science Review*, 2025.
[48] A. O. Ajayi-Nifise, T. Falaiye, O. Olubusola, A. I. Daraojimba, and N. Z. Mhlongo, "Blockchain in us accounting: A review: Assessing its transformative potential for enhancing transparency and integrity," *Finance & Accounting Research Journal*, vol. 6, no. 2, pp. 159–182, 2024.
[49] R. Karim and I. Sifat, "Blockchain technology in the energy industry: a review on policies and regulations," *Blockchain Technology*, pp. 109–126, 2022.
[50] A. Ferreira da Silva, A. C. Moxoto, and E. Mota, "Blockchain and the future of credit: An overview of p2p platforms and their potential impacts," *Available at SSRN 5065160*.
[51] H. Sadri, I. Yitmen, L. C. Tagliabue, F. Westphal, A. Tezel, A. Taheri, and G. Sibenik, "Integration of blockchain and digital twins in the smart built environment adopting disruptive technologies—a systematic review," *Sustainability*, vol. 15, no. 4, p. 3713, 2023.
[52] B. S. Samantray and K. Reddy, "Blockchain-enabled secured supply chain for smart cities: A systematic review on architecture, technology, and service management," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, pp. 1–31, 2025.
[53] H. Kim, Z. Xiao, X. Zhang, X. Fu, and Z. Qin, "Rethinking blockchain technologies for the maritime industry: An overview of the current landscape," *Future Internet*, vol. 16, no. 12, p. 454, 2024.
[54] W. Rafique and J. Qadir, "Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain," *Computer Science Review*, vol. 54, p. 100678, 2024.
[55] H. S. Musa, M. Krichen, A. A. Altun, and M. Ammi, "Survey on blockchain-based data storage security for android mobile applications," *Sensors*, vol. 23, no. 21, p. 8749, 2023.
[56] S. Ngusoon and S. N. Agwaza, "Integrating artificial intelligence in estate management: Innovations, challenges, and future prospects," *Applied Sciences, Computing, and Energy*, vol. 1, no. 1, pp. 63–85, 2024.
[57] S. Qiang, "Integration of blockchain in ai-driven trade facilitation: Challenges and opportunities," *Journal of AI-Driven Trade Facilitation Engineering and Single Window Systems*, vol. 2, no. 1, pp. 35–61, 2024.
[58] N. Afrin and A. Pathak, "Blockchain-powered security and transparency in supply chain: Exploring traceability and authenticity through smart contracts," *International Journal of Computer Applications*, vol. 85, pp. 5–15, 2023.
[59] S. H. Mousavi, A. Tohidinia, and S. M. Mousavi, "Transforming islamic finance: the impact of blockchain and smart sukuk," *Access Journal*, vol. 6, no. 1, pp. 184–201, 2025.
[60] P. Chatterjee, "Blockchain technology as the backbone of fintech innovation: Opportunities and challenges," *International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN*, pp. 2349–5162, 2023.
[61] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in iot cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.