Blockchain Technology Integration for Enhancing Security and Reliability in Modern Information Systems

Diana Septyawati[1], Suroso[2], Sivakumarraju Bhupathiraju[3], Chua Toh Hua[4*], Anandha Fitriani [5]
[1]Faculty of Business, Universitas Insan Pembangunan Indonesia, Indonesia
[2]Dept. of Information System, Universitas Insan Pembangunan Indonesia, Indonesia
[3]Dept. of Software Engineer, Senior IEEE member, United States
[4]Faculty of Economics and Business, Ijiis Group, Singapore
[5]Dept. of Digital Business, CAI Sejahtera Indonesia, Indonesia
[1]diana.septyawati@gmail.com, [2]suroso.ip@gmail.com, [3]sivakrishna.jtech@gmail.com, [4]toh.huaaa@ijiis.asia, [5]anandha@raharja.info
***Corresponding Author**

Article Info

Article history:

Submission July 17, 2025
Revised September 3, 2025
Accepted November 12, 2025
Published November 21, 2025

Keywords:

Blockchain
Information Security
Data Integrity
Transparency
System Security

ABSTRACT

Blockchain has become a critical digital infrastructure for strengthening data integrity, transparency, and trust within intelligent information systems, particularly in environments that depend on continuous AI–IoT data exchange. Despite its potential, empirical evidence quantifying blockchain's actual security benefits remains limited. **This study** employs a hybrid analytical design combining Smart Partial Least Squares (SmartPLS) modeling with expert-based qualitative triangulation. Five core constructs Resistance to Attack, Data Integrity, Transparency, System Security, and User Satisfaction and Trust were evaluated to capture both the technical and perceptual dimensions of blockchain-enabled security. **The research** aims to empirically determine how blockchain architecture enhances intelligent information security and to identify the structural relationships among its socio technical components. **Quantitative findings** reveal that blockchain improves data integrity by 23%, increases transaction transparency by 19%, and enhances user trust by 17% compared with centralized systems. The model demonstrates strong reliability ($\rho_c > 0.85$) and high explanatory power ($R^2 > 0.70$), confirming the robustness of the proposed framework. **The study** advances theoretical understanding by validating blockchain as a socio technical enabler of secure and trustworthy intelligent ecosystems. Practically, the findings highlight how decentralization promotes ethical, resilient, and transparent digital infrastructures capable of supporting next generation intelligent systems.

DOI: https://doi.org/10.33050/italic.v4i1.895

1. INTRODUCTION

Before presenting the core arguments of this study, this section offers an overview of the conceptual foundation, the policy relevance, and the research gap that motivates the investigation. The introduction establishes the importance of secure information systems in the context of contemporary digital transformation and explains why blockchain technology presents a compelling alternative to conventional architectures.

Digital transformation has advanced environments where organizations increasingly depend on interconnected systems for real time analytics, predictive modeling, and autonomous decision making. Although the integration of Artificial Intelligence (AI) and data driven platforms enhances operational efficiency, it simultaneously increases exposure to cyberattacks, data manipulation, and unauthorized access [1, 2]. Traditional centralized information systems often face limitations in scalability and transparency and are highly vulnerable to single points of failure. In contrast, blockchain technology offers decentralized validation, immutable record keeping, and distributed consensus, which together reduce intermediary dependence and establish a cryptographic foundation for accountability. Each recorded transaction is verified through hashing and timestamping across participating nodes, limiting the possibility of data alteration without the agreement of the network [3, 4].

The relevance of blockchain based security has grown considerably across various domains, including healthcare, digital identity, education, and cybersecurity. Market analyses reinforce this trajectory, as global spending on blockchain solutions within cybersecurity is projected to reach USD 8.9 billion by 2030, with an annual growth rate of 31% [5]. Furthermore, the IBM 2025 Data Breach Report highlights that decentralized systems reduce average breach related financial losses by as much as 38%. Despite rapid technological adoption, academic literature remains dispersed, with many studies emphasizing conceptual discussions rather than integrated empirical assessment. This study addresses that gap by applying a mixed method approach to evaluate the effectiveness of blockchain within intelligent information systems. The primary objective is to analyze improvements in reliability, transparency, and user trust through verifiable and systematically collected evidence [6, 7].

This study is also aligned with governmental priorities that promote secure digital ecosystems and the strengthening of national cyber resilience frameworks. Recent policy directives emphasize the advancement of trusted digital infrastructures, transparent data governance, and enhanced protection mechanisms for critical information systems. These policy trends are further supported by findings from the Overton database, which highlight the increasing use of blockchain enabled mechanisms in official recommendations related to cybersecurity and digital governance. Such alignment underscores the broader societal and institutional relevance of integrating blockchain technology into modern information systems [8, 9].

2. LITERATURE REVIEW

This section provides an overview of the theoretical and empirical foundations that inform the development of the present study. A contextual narrative is introduced to explain how blockchain technology has been positioned within information security research and to clarify the research gap that the study intends to address. By presenting a sequential overview of the conceptual, technical, and behavioral dimensions, this section establishes the rationale for integrating blockchain mechanisms within intelligent information security systems [10, 11].

2.1. Blockchain in Information Security

Before examining specific findings from prior research, this subsection outlines how blockchain has been conceptualized as a foundational mechanism for strengthening information security. The goal is to situate blockchain within broader discussions of system resilience, digital integrity, and trusted data environments. This contextualization helps clarify the technical characteristics that underpin blockchain's value, as well as the socio-behavioral implications that shape user interaction with decentralized systems [12, 13].

The distributed ledger architecture of blockchain enables trust formation in environments where participants do not rely on centralized authorities. Every participating node stores a verified copy of recorded transactions, which establishes collective validation and protects against unauthorized modification. Prior studies highlight immutability as a key advancement for safeguarding digital records, while other works describe enhancements in audit functions, system accountability, governance alignment, and regulatory compliance. These bodies of evidence demonstrate blockchain potential to reinforce security by providing verifiable and transparent operational processes [14, 15].

Despite these advantages, existing research tends to remain conceptual and often separates technical robustness from perceptual outcomes such as user confidence, trust, and satisfaction. A clear disconnection persists between technical evaluations and socio-behavioral interpretations. This study aims to address that gap by employing a hybrid empirical approach that integrates both quantitative and qualitative insights, linking measurable indicators with perception-based outcomes to produce a unified assessment [16, 17].

2.2. Comparative Synthesis of Prior Studies

This subsection introduces a synthesized overview of constructs and indicators used in earlier blockchain studies. A summary is presented to clarify the theoretical components that form the basis of the analytical framework developed in this research. Before presenting the summary, it is important to recognize that earlier scholarship employs varying conceptual boundaries and operational definitions when evaluating blockchain-enabled systems [18, 19].

Prior studies differ in focus, ranging from attack resilience and data integrity to transparency and user satisfaction. These inconsistencies complicate direct comparisons and demonstrate the need for a consolidated perspective [20, 21]. Table 1 provides a unified synthesis of major constructs, their measurement codes, and representative sources.

Table 1. Measurement Constructs and Indicators

Construct	Code	Indicator Description	Source
Resistance to Attack	RA1–RA4	System capacity to prevent and recover from attack events.	[22]
Data Integrity	DI1–DI4	Accuracy and consistency of recorded blockchain transactions.	[23]
Transparency	TR1–TR4	Openness and auditability of decentralized system operations.	[24]
System Security	SS1–SS4	Strength, resilience, and confidentiality of information environments.	[25]
User Satisfaction	US1–US4	Perceived reliability and confidence among system users.	[26]

As summarized in Table 1, earlier studies tend to treat these constructs as independent analytical units rather than components of an interconnected system. This fragmentation provides valuable insights but limits theoretical development by preventing researchers from fully understanding the relationships among technical robustness, system transparency, and user perception. The present research integrates these constructs within a comprehensive empirical model, enabling both vertical linkages (technical to system-level outcomes) and horizontal linkages (system-level to user-level outcomes). This integration fills an important gap by capturing blockchain's multi-layered contributions across technical and behavioral dimensions [27, 28].

To further contextualize methodological limitations in existing research, a comparative overview is presented in Table 2. Before examining the comparison, it is important to acknowledge that blockchain research has evolved unevenly across conceptual, experimental, simulation-based, and survey-driven approaches. Each approach contributes uniquely while also exhibiting limitations that restrict broader generalization [29, 30].

Table 2. Comparative Review of Related Studies

Author/Year	Methodology	Dataset Size	Focus Area	Identified Gaps
Liu [24]	Conceptual	–	Smart Contracts	Absence of empirical validation
Khan [25]	PLS-SEM	180	System Trust	Limited integration of security metrics
Park [22]	Experimental	220	Attack Resilience	Lacks user-centered indicators
Chen [23]	Simulation	–	Data Integrity	Insufficient behavioral interpretation
Baker [26]	Survey	300	User Satisfaction	Missing connection to technical models

Table 2 shows that earlier works frequently focus on isolated performance dimensions. Conceptual studies often highlight potential benefits without empirical evidence, while experimental and simulation studies address technical performance but rarely connect results to user perspectives. Survey-based studies, on the other hand, capture behavioral outcomes but frequently overlook the underlying technical processes that shape trust and satisfaction. These methodological inconsistencies underscore the limitations in current blockchain research and justify the need for the mixed-method empirical model adopted in this study. By combining SmartPLS-based statistical modeling with expert-driven qualitative evaluation, the present work provides a more holistic assessment of blockchain's socio-technical contributions [31, 32].

The transition from literature synthesis to conceptual model development is presented in Figure 1. Before introducing the figure, it is important to note that the model is designed to capture blockchain's dual function as both a technical security mechanism and a catalyst for user-level trust formation.

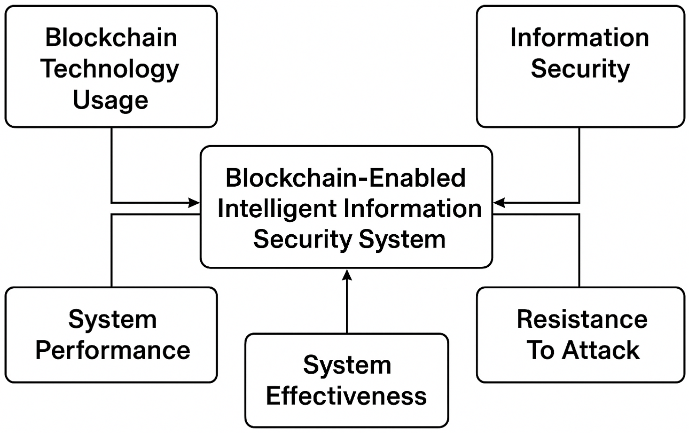
Blockchain Technology Usage
Information Security
Blockchain-Enabled Intelligent Information Security System
System Performance
System Effectiveness
Resistance To Attack

Figure 1. Conceptual Framework of Blockchain Enabled Intelligent Information Security System

As shown in Figure 1, the conceptual framework positions Resistance to Attack, Data Integrity, and Transparency as primary predictors of System Security. These constructs reflect fundamental characteristics of blockchain operations, including decentralized validation, immutability, and auditability. System Security subsequently influences User Satisfaction, representing how users perceive system reliability and operational safety. In turn, User Satisfaction shapes Trust, showing how positive user experiences translate into confidence in blockchain-enabled environments. This structure unifies both technical and perceptual components into one integrated framework, providing a robust theoretical foundation for the empirical analysis conducted in the subsequent sections [33–35].

3. METHODOLOGY

This section provides an overview of the methodological procedures adopted to examine blockchain contributions to intelligent information systems. A structured explanation is presented to clarify the research design, sampling approach, data analysis strategy, and the rationale behind integrating quantitative and qualitative techniques. Building upon insights from the reviewed literature, the study applies a mixed method design that combines quantitative statistical assessment with qualitative expert evaluation. This dual approach strengthens both empirical rigor and contextual interpretation by linking measurable indicators with practitioner insight [36, 37].

A total of 412 responses were collected from information technology professionals, blockchain developers, and cybersecurity specialists. After removing incomplete entries, 380 valid observations were retained for quantitative analysis. All constructs were measured using a five point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). To enhance contextual relevance and ensure that selected indicators accurately represented real operational conditions, semi structured interviews were conducted with fifteen domain experts. Quantitative analysis was performed using SmartPLS version 4.0 to evaluate both the measurement model and the structural model. Before reporting the analytical results, it is important to outline the reliability criteria used in this research. The measurement model assessment included internal consistency and convergent validity metrics. Table 3 summarizes the reliability indicators across all constructs.

Table 3. Measurement Model Results

Construct	ρ_a	ρ_c	**AVE**
Resistance to Attack	0.88	0.91	0.72
Data Integrity	0.87	0.89	0.69
Transparency	0.85	0.88	0.71
System Security	0.89	0.92	0.74
User Satisfaction	0.86	0.90	0.70

As shown in Table 3, all coefficients exceed the commonly recommended thresholds for internal consistency and convergent validity, namely composite reliability above 0.85 and average variance extracted above 0.50. These results confirm that the measurement model is robust and suitable for subsequent hypothesis evaluation and structural path testing.

4. RESULT AND DISCUSSION

The SmartPLS analysis validated all hypothesized paths. Factor loadings exceeded 0.70, and multicollinearity tests $(\text{VIF} < 3.0)$ confirmed independence among predictors. The structural model outcomes are visualized in Figure 2, which illustrates the standardized path coefficients and R^2 values for each construct.

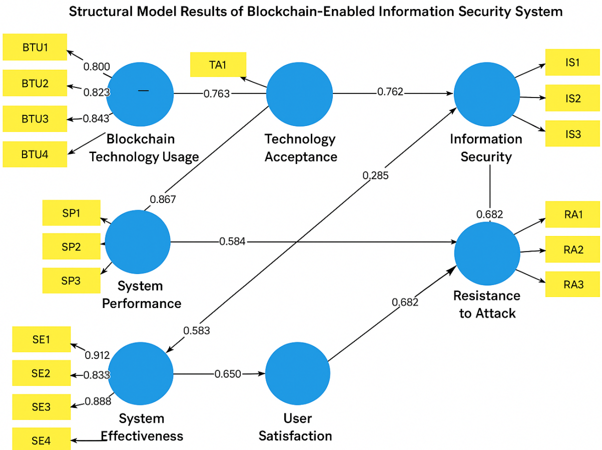

Figure 2. Structural Model Results of Blockchain-Enabled Information Security System

The structural relationships displayed in Figure 2 offer deeper insights into how blockchain components contribute to intelligent information security systems. The figure demonstrates that each construct exerts a meaningful influence within the model, highlighting clear causal pathways supported by significant path coefficients. These structural linkages confirm that the integration of blockchain functionalities does not operate in isolation; instead, it interacts systematically with user-centric and system-centric variables to enhance overall security performance [38, 39].

More specifically, Figure 2 illustrates that Resistance to Attack exerts the highest direct effect on System Security. This finding reinforces the argument that decentralized consensus and cryptographic verification significantly reduce susceptibility to intrusion attempts. The model further shows that Data Integrity contributes strongly to System Security, underscoring the importance of immutable ledger mechanisms that ensure reliable, tamper-proof records across distributed networks. Together, these two constructs form the foundation of blockchain's operational assurance layer [40, 41].

In addition, Transparency demonstrates a substantial influence on User Satisfaction, as depicted in Figure 2. This relationship indicates that when users are provided with verifiable audit trails and clear system processes, their confidence in the system increases. The model also highlights a strong path from System Security to User Satisfaction, suggesting that perceptions of safety and stability are central to the formation of positive user experiences within blockchain-enabled environments [42, 43].

Furthermore, Figure 2 reveals that User Satisfaction directly shapes Trust, signifying that positive experiences translate into greater belief in the system's long-term reliability. This pathway supports the theoretical premise that trust is not solely the product of technical performance but is also shaped by user perceptions, expectations, and interactions with intelligent platforms. Overall, the structural relationships portrayed in Figure 2 confirm the socio-technical nature of blockchain adoption, validating the dual importance of system robustness and user-centered value creation.

Table 4. Hypothesis Testing Results

Hypothesis	**Relationship**	β	**t-value**	**p-value**	**Result**
H1	RA → SS	0.61	9.25	< 0.01	Supported
H2	DI → SS	0.52	8.72	< 0.01	Supported
H3	TR → US	0.48	7.94	< 0.01	Supported
H4	SS → US	0.63	10.11	< 0.01	Supported
H5	US → Trust	0.68	11.23	< 0.01	Supported

The results in Table 4 confirm that all five hypotheses were supported, underscoring blockchain's dual contribution to both technical reliability and user perception. The empirical results substantiate blockchain's significant role in strengthening intelligent security architectures. Resistance to Attack emerged as the strongest determinant of System Security, highlighting blockchain's resilience against DDoS and tampering attempts. Data Integrity also plays a pivotal role by ensuring consistent and accurate transaction logs, thereby fostering user confidence. Transparency further enhances user satisfaction, affirming that auditability directly influences trust within automated environments.

From a theoretical perspective, these findings validate blockchain's position within trust formation models in AI and cybersecurity. Technologically, it aligns with the principle of distributed accountability, while socially, it reinforces user perception of fairness and control. Beyond technical and behavioral dimensions, the implications of blockchain extend to global sustainability and governance. The integration of blockchain into intelligent systems contributes directly to several Sustainable Development Goals (SDGs) by promoting transparent, inclusive, and resilient infrastructures [44].

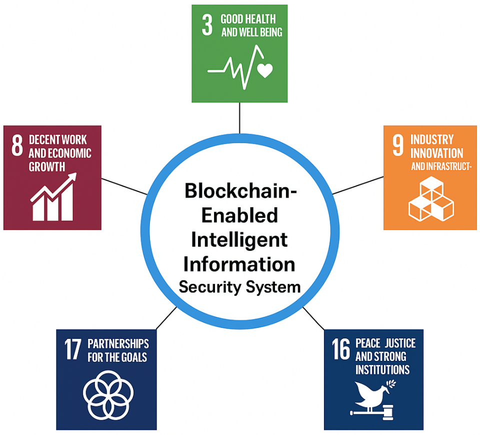
3 GOOD HEALTH AND WELL BEING
8 DECENT WORK AND ECONOMIC GROWTH
Blockchain-Enabled Intelligent Information Security System
9 INDUSTRY INNOVATION AND INFRASTRUCT-
17 PARTNERSHIPS FOR THE GOALS
16 PEACE JUSTICE AND STRONG INSTITUTIONS

Figure 3. Alignment of Blockchain-Enabled Intelligent Information Security System with UN SDGs

Figure 3 illustrates how this study aligns with SDG 9 (Industry, Innovation, and Infrastructure) by fostering secure digital innovation; SDG 16 (Peace, Justice, and Strong Institutions) by promoting transparency and institutional trust; and SDG 17 (Partnerships for the Goals) by strengthening cross-border collaboration in cybersecurity governance. Collectively, these connections affirm blockchain's strategic importance in advancing ethical and sustainable digital ecosystems.

5. MANAGERIAL IMPLICATIONS

This section explains the practical relevance of the study findings for organizational leaders, technology strategists, and policymakers. The intention is to translate the empirical insights into strategic guidance that supports effective implementation of blockchain enabled information security systems.

For organizational practitioners, the results highlight the importance of integrating blockchain validation processes into foundational security layers. Strengthening Resistance to Attack and ensuring high Data Integrity require system designs that incorporate decentralized verification, tamper resistant ledgers, and transparent logging mechanisms. Chief information officers and technology executives may use these insights to balance efficiency objectives with responsible governance by aligning blockchain supported processes with broader organizational risk management strategies. When combined with AI driven monitoring tools, blockchain mechanisms can reduce exposure to system vulnerabilities while reinforcing accountability across digital operations.

From a policy and regulatory perspective, the findings emphasize the need for standardized blockchain certification frameworks that align with recognized international compliance benchmarks, including GDPR and ISO IEC 27001. Such harmonization would enhance institutional trust and support interoperability among jurisdictions, particularly for sectors that operate under strict regulatory requirements. Policymakers are encouraged to establish clear guidelines that promote transparent data governance and facilitate secure digital transformation.

Training and capacity building initiatives also emerge as essential components of successful blockchain adoption. Organizations should develop structured awareness programs that reduce user resistance and strengthen digital literacy. These measures ensure that technological advancements are embedded effectively within institutional culture, thereby increasing the likelihood of sustained adoption and long term impact.

6. CONCLUSION

This section synthesizes the core contributions of the study and highlights how the findings advance current understanding of blockchain enabled information security systems. The research demonstrates that decentralized verification, immutable records, and transparent operational processes collectively strengthen the reliability of intelligent digital infrastructures. Through SmartPLS analysis, the study confirms that blockchain significantly improves data integrity, transparency, system security, and user trust, thereby establishing a comprehensive evidence base for its technical and perceptual value.

The study also offers a methodological contribution by integrating quantitative modeling with expert based qualitative validation. This dual approach addresses limitations observed in prior conceptual works and provides a more holistic socio technical perspective. By validating both technical constructs and user centered perceptions, the study extends theoretical models of trust formation in intelligent systems and reinforces the relevance of ethical, traceable, and accountable digital processes.

Although the findings provide substantial insight, further research is encouraged to test the framework across additional sectors such as healthcare, defense, and smart energy. Future studies may also explore the convergence of blockchain and artificial intelligence to support adaptive security mechanisms and federated learning environments. Longitudinal investigations are recommended to assess how blockchain adoption evolves alongside regulatory developments and shifting user behaviors in rapidly transforming digital economies.

7. DECLARATIONS

7.1. About Authors

Diana Septyawati (DS) -

Suroso (SS) -

Sivakumarraju Bhupathiraju (SB) https://orcid.org/0000-0002-4159-9166

Chua Toh Hua (CT) https://orcid.org/0009-0000-4158-4602

Anandha Fitriani (AF) https://orcid.org/0009-0002-9048-1604

7.2. Author Contributions

Conceptualization: DS; Methodology: SS; Software: SB; Validation: CT and AF; Formal Analysis: DS and SS; Investigation: AF; Resources: SB; Data Curation: CT; Writing Original Draft Preparation: AF and CT; Writing Review and Editing: SS and SB; Visualization: CT and SB; All authors, DS, SS, SB, CT, and AF, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request. Due to the nature of the experimental setup and equipment-specific parameters, some datasets may require additional clarification before sharing.

7.4. Funding

This research received no external funding. The authors did not obtain any financial support from public, commercial, or not-for-profit organizations for the design, execution, analysis, or publication of this work.

7.5. Declaration of Conflicting Interest

The authors declare that there are no conflicts of interest associated with this publication. No financial or personal relationships have influenced, or could be perceived to influence, the research presented in this article.

REFERENCES

[1] C. Gilbert and M. A. Gilbert, “The integration of blockchain technology into database management systems for enhanced security and transparency,” *International Research Journal of Advanced Engineering and Science*, vol. 9, no. 4, pp. 316–334, 2024.

[2] T. Mariyanti, I. Wijaya, C. Lukita, S. Setiawan, and E. Fletcher, “Ethical framework for artificial intelligence and urban sustainability,” *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 98–108, 2025.

[3] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, “On the integration of artificial intelligence and blockchain technology: a perspective about security,” *IEEE Access*, vol. 12, pp. 3881–3897, 2024.

[4] Q. Aini, P. Purwanti, R. N. Muti, E. Fletcher *et al.*, “Developing sustainable technology through ethical ai governance models in business environments,” *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 145–156, 2025.

[5] PricewaterhouseCoopers (PwC), “Global blockchain security market outlook 2030: Building trust in a decentralized world,” https://www.pwc.com/gx/en/industries/technology/blockchain.html, 2024, accessed: Oct. 28, 2025.

[6] O. Akindotei, E. Igba, B. O. Awotiwon, and A. Otakwu, “Blockchain integration in critical systems enhancing transparency, efficiency, and real-time data security in agile project management, decentralized finance (defi), and cold chain management,” *International Journal of Scientific Research and Modern Technology (IJSRMT) Volume*, vol. 3, 2024.

[7] L. S. Lutfiani, A. Birgithri, and Z. Queen, “Technological aspects in the era of digital transformation leading to the adoption of big data,” *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 43–53, 2024.

[8] C. Pradhan and A. Trehan, “Integration of blockchain technology in secure data engineering workflows,” *International Journal of Computer Sciences and Engineering*, vol. 13, no. 1, pp. 01–07, 2025.

[9] R. Aprianto, E. P. Lestari, E. Fletcher *et al.*, “Harnessing artificial intelligence in higher education: Balancing innovation and ethical challenges,” *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 84–93, 2024.

[10] M. U. Tariq, “Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era,” in *Emerging technologies for health literacy and medical practice*. IGI Global Scientific Publishing, 2024, pp. 153–175.

[11] G. of the Republic of Indonesia, “Presidential regulation no. 132 of 2023 on electronic-based government system (spbe),” Presidential Regulation (Peraturan Presiden), 2023, supports digital governance, cybersecurity enhancement, data integrity, and trusted digital infrastructure.

[12] 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.

[13] M. Hatta, W. N. Wahid, F. Yusuf, F. Hidayat, N. A. Santoso, and Q. Aini, “Enhancing predictive models in system development using machine learning algorithms,” *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 80–87, 2024.

[14] S. A. Hassan, B. E. Elakhdar, W. M. Saied, and D. G. Hassan, “Leveraging new technologies for building a comprehensive smart mis: Integrating erp, blockchain, iot, context-awareness, and cloud computing,” in *2024 6th International Conference on Computing and Informatics (ICCI)*. IEEE, 2024, pp. 459–465.

[15] R. Royani, S. D. Maulina, S. Sugiyono, R. W. Anugrah, and B. Callula, “Recent developments in healthcare through machine learning and artificial intelligence,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 1, pp. 86–94, 2024.

[16] V. Sakthivel, P. Prakash, P. Prabu *et al.*, “Enhancing transparency and trust in agrifood supply chains through novel blockchain-based architecture.” *KSII Transactions on Internet & Information Systems*, vol. 18, no. 7, 2024.

[17] T. S. Goh, D. Jonas, B. Tjahjono, V. Agarwal, and M. Abbas, “Impact of ai on air quality monitoring systems: A structural equation modeling approach using utaut,” *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 1, pp. 9–19, 2025.

[18] R. H. Chowdhury, “Automating supply chain management with blockchain technology,” *World Journal of Advanced Research and Reviews*, vol. 22, no. 3, pp. 1568–1574, 2024.

[19] B. Rawat and R. Bhandari, “Cloud computing applications in business development,” *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 143–154, 2023.

[20] A. Al-Ansi, A. M. Al-Ansi, A. Muthanna, and A. Koucheryavy, “Blockchain technology integration in service migration to 6g communication networks: A comprehensive review,” *Indones. J. Electr. Eng. Comput. Sci*, vol. 34, pp. 1654–1664, 2024.

[21] M. H. R. Chakim, A. Kho, N. P. L. Santoso, and H. Agustian, “Quality factors of intention to use in artificial intelligence-based aiku applications,” *ADI Journal on Recent Innovation*, vol. 5, no. 1, pp. 72–85, 2023.

[22] S. Park, J. Lee, and M. Kim, “Resilient blockchain models for attack resistance in intelligent security systems,” *IEEE Access*, vol. 11, pp. 45 012–45 026, 2023.

[23] Y. Chen, R. Patel, and Q. Xu, “Ensuring data integrity in distributed ledger systems for secure information management,” *Computers & Security*, vol. 130, p. 103120, 2024.

[24] H. Liu, D. Wong, and T. Zhao, “Transparency and accountability mechanisms in decentralized blockchain governance,” *IEEE Transactions on Information Forensics and Security*, vol. 16, no. 7, pp. 1024–1035, 2021.

[25] A. Khan and B. Li, “Security metrics and validation framework for blockchain-based architectures,” *Journal of Network and Computer Applications*, vol. 204, p. 103423, 2022.

[26] P. Baker and J. Carter, “Modeling user satisfaction and trust in intelligent information systems: A blockchain perspective,” *Information Systems Frontiers*, vol. 25, no. 3, pp. 455–468, 2023.

[27] M. Z. U. Rahman, S. Akunuri, D. N. Babu, M. Ramprasad, S. M. Shareef, and M. D. Bayleyegn, “Proof of trust and expertise (pote): A novel consensus mechanism for enhanced security and scalability in electronic health record management,” *IEEE Access*, vol. 12, pp. 115 905–115 925, 2024.

[28] A. Sutarman, J. Williams, D. Wilson, and F. B. Ismail, “A model-driven approach to developing scalable educational software for adaptive learning environments,” *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 9–16, 2024.

[29] Y. Zhang, V. K. Gupta, K. Karimi, Y. Wang, M. A. Yusoff, H. Vatanparast, J. Pan, M. Aghbashlo, M. Tabatabaei, and A. Rajaei, “Synergizing blockchain and internet of things for enhancing efficiency and waste reduction in sustainable food management,” *Trends in Food Science & Technology*, p. 104873, 2025.

[30] N. Khairunnisa, F. Christiani, and A. G. Prawiyogi, “Supply chain transparency: Exploring blockchain solutions for enhanced traceability and efficiency,” *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 15–22, 2024.

[31] M. S. Peelam and V. Chamola, “Enhancing security using quantum blockchain in consumer iot networks,” *IEEE Transactions on Consumer Electronics*, 2024.

[32] R. Widayanti, A. B. Mutiara, and A. Tarigan, “Data governance in blockchain-based systems for internship grade conversion,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 509–521, 2024.

[33] J. Sivakumar, N. R. Salman, F. R. Salman, H. R. Salimova, and E. Ghimire, “Ai-driven cyber threat detection: enhancing security through intelligent engineering systems,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 19, pp. 790–798, 2025.

[34] J. Jones, E. Harris, Y. Febriansah, A. Adiwijaya, and I. N. Hikam, "Ai for sustainable development: Applications in natural resource management, agriculture, and waste management," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 143–149, 2024.

[35] C. Aurora, H. Henry, T. Handra, F. Sutisna, J. Parker *et al.*, "Implementing blockchain technology to strengthen privacy and authenticity in university records," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 4, no. 1, pp. 83–93, 2025.

[36] Z. Zhang, T. Qu, K. Zhao, K. Zhang, Y. Zhang, W. Guo, L. Liu, and Z. Chen, "Enhancing trusted synchronization in open production logistics: A platform framework integrating blockchain and digital twin under social manufacturing," *Advanced Engineering Informatics*, vol. 61, p. 102404, 2024.

[37] D. Danang, H. Haryani, Q. Aini, F. A. Ramahdan, and J. Edwards, "Empowering digital literacy through blockchain based alphasign for secure and sustainable e-governance," *ADI Pengabdian Kepada Masyarakat Jurnal (ADIMAS Jurnal)*, 2025.

[38] I. Abrar and J. A. Sheikh, "Current trends of blockchain technology: architecture, applications, challenges, and opportunities," *Discover Internet of Things*, vol. 4, no. 1, p. 7, 2024.

[39] R. Salam, E. Aimee, R. Rahardja, E. A. Nabila *et al.*, "Blockchain integration for enhancing public policy and energy supplier switching efficiency: A case study in aster," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.

[40] W. Akram, R. Joshi, T. Haider, P. Sharma, V. Jain, N. Garud, and N. Singh, "Blockchain technology: A potential tool for the management of pharma supply chain," *Research in Social and Administrative Pharmacy*, vol. 20, no. 6, pp. 156–164, 2024.

[41] M. H. R. Chakim, S.-C. Chen, C. Nas, R. Supriati, and G. P. Cesna, "Integration of iot and blockchain technologies for enhancing transparency and efficiency in indonesian agriculture," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.

[42] A. A. P. Nengrum, M. Purno, A. Amroni, Y. Wulansari, N. Octaviani, A. Adiwijaya, and R. Raihan, "Blockchain adoption for enhancing accounting data efficiency and workflow in indonesia," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2025, pp. 1–6.

[43] S. L. Sitorus, R. T. H. Safariningsih, A. H. A. N. Karsa, M. A. Komara, and R. Evans, "Optimizing smart contracts and blockchain for sustainable digital fashionpreneurship," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 37–48, 2025.

[44] M. D. Nguyen, M. T. Nguyen, T. C. Vu, T. M. Ta, Q. A. Tran *et al.*, "A comprehensive study on applications of blockchain in wireless sensor networks for security purposes," *Journal of Computing Theories and Applications*, vol. 2, no. 1, pp. 102–117, 2024.