Blockchain Frontier Technology (B-Front)
Vol. 5, No. 2, 2026, pp. 219∼229
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

Governance Models for Blockchain Integrated IoT Ecosystems

Rizki Indrawan[1], Arista Ratih[2], Harry Agustian[3*], Richard Evans[4]
[1]Department of Accounting, Universitas Kuningan, Indonesia
[2]Bachelor of Biology Education, Universitas Merangin, Indonesia
[3]Department of Computer System, Seni Sejahtera Indonesia, Indonesia
[4]Master of Information Technology, Adi-Journal Incorporation, United States
[1]rizki.indrawan@uniku.ac.id, [2]aristaratih92@gmail.com, [3]harry.agustian@raharja.info, [4]vans.richard@adi-journal.org
***Corresponding Author**

Article Info

Article history:

Submission, 14-11-2025
Revised, 30-12-2025
Accepted, 10-01-2026

Keywords:

Blockchain
IoT
Governance
Smart Contract
Decentralization

ABSTRACT

The rapid advancement of the Internet of Things (IoT) has led to the creation of large-scale interconnected networks of smart devices capable of autonomously collecting, processing, and exchanging data in real time across diverse application domains. While this development offers significant benefits, it also introduces critical challenges related to data security, privacy protection, interoperability, and the increasingly complex governance of distributed IoT systems. Traditional centralized governance approaches often fail to address these issues effectively due to single points of failure, limited transparency, and insufficient trust mechanisms. The integration of blockchain technology into IoT ecosystems provides a promising alternative by leveraging decentralized architecture, immutable ledgers, transparency, and tamper-resistant features that enhance accountability and trust. **This study aims** to identify and design an appropriate governance model for blockchain-integrated IoT systems that balances security, operational efficiency, and decentralization. **The research** adopts a conceptual and qualitative approach through a systematic literature analysis and the synthesis of existing governance, blockchain, and IoT frameworks to develop a structured governance model. The proposed framework defines institutional roles, policy structures, decision-making processes, and control mechanisms among participating entities. **The results** demonstrate that a blockchain-based governance model enhances system security, operational efficiency, and inter-organizational trust by reducing reliance on centralized authorities and improving data integrity. In addition, the use of smart contracts enables automated policy enforcement, transparent coordination, and sustainable system operations, supporting scalable and resilient governance for future blockchain–IoT ecosystems.

DOI: https://10.34306/bfront.v5n2.974

1. INTRODUCTION

The rapid development of digital technology has accelerated the growth of the Internet of Things (IoT), a network of smart devices capable of collecting, processing, and exchanging data through the internet. The number of IoT devices worldwide is projected to reach 30 billion by 2030, underscoring its increasingly critical

role across sectors such as industry, transportation, healthcare, and smart city management [1]. In recent years, IoT systems have increasingly been designed as large-scale distributed and Cyber-Physical Systems (CPS), integrating physical processes with computation, communication, and control. These systems follow emerging standards to ensure interoperability, reliability, and security across heterogeneous devices [2, 3, 4]. As a result, IoT governance must address not only data management concerns but also engineering challenges, including standard compliance, distributed coordination, and CPS dependability. Despite these advances, most existing IoT infrastructures still rely on centralized cloud-based architectures, which introduce persistent challenges related to data security, privacy, and system governance [5].

To address these limitations, blockchain technology has emerged as a promising solution. Blockchain enables decentralized, transparent, and tamper-resistant data recording through distributed verification among network nodes, thereby enhancing security and trust in data exchange among IoT devices [6, 7]. Furthermore, the implementation of smart contracts allows device authentication and operational processes to be executed automatically without the involvement of third-party intermediaries, improving both efficiency and reliability.

However, the integration of blockchain into IoT systems introduces new governance challenges. In the absence of a central authority, blockchain-integrated IoT ecosystems require alternative governance models capable of regulating roles, responsibilities, and decision-making processes without undermining decentralization or system efficiency [8, 9, 10].

Accordingly, this study focuses on designing an appropriate governance model for blockchain-integrated IoT ecosystems. This research is guided by two main questions.

- How can governance mechanisms be structured to balance decentralization, security, and operational efficiency in blockchain-integrated IoT systems?
- How can technical automation and human oversight be effectively combined to ensure accountability within distributed cyber-physical systems?

The proposed governance model is expected to address emerging challenges related to security, transparency, and stakeholder coordination resulting from the integration of blockchain and IoT technologies.

Table 1 illustrates how blockchain implementation can address the primary weaknesses of traditional IoT systems, particularly with respect to security, trust, and data management transparency. The table highlights key differences between traditional IoT systems and blockchain-based IoT systems in terms of operational structure, transparency, efficiency, and scalability [11].

Table 1. Comparison Between Traditional IoT Systems and Blockchain-Based IoT Systems

Aspect	**Traditional IoT**	**Blockchain-Based IoT**
System Structure	Centralized Server	Distributed Ledger
Data Security	Relies on a central server	Secured through cryptography and consensus
User Privacy	Vulnerable to data breaches	More secure due to encryption and anonymity
System Transparency	Limited to the managing entity	Can be verified by all network participants
Operational Efficiency	Prone to bottlenecks under heavy load	Automated processes through smart contracts
Network Scalability	Depends on server capacity	Can be expanded through a global node network

Table 1 further illustrates the fundamental differences between conventional IoT systems and blockchain-integrated IoT systems. In traditional IoT environments, data storage and decision-making processes are largely controlled by centralized servers, which increases vulnerability to system failures and cyberattacks. Multiple nodes and transactions are verified collectively, in contrast blockchain–IoT systems operate in a decentralized manner, where data are not stored in a single location but distributed across multiple nodes. Each transaction is verified collectively by the network, which helps reduce dependency on central servers and increases system robustness [12].

The growth of IoT technology has resulted in a highly interconnected digital environment, with millions of devices exchanging data automatically on a continuous basis. While this development creates new opportunities for efficiency and innovation, it also brings serious challenges related to security, privacy, and data management. Blockchain integration is often viewed as a practical response to these challenges because it introduces transparent data handling, stronger security mechanisms, and reduced reliance on a single controlling authority. However, decentralization also introduces governance concerns. Unlike conventional systems with centralized oversight, blockchain–IoT networks do not have a single entity responsible for supervising operations and resolving coordination issues across the ecosystem [13, 14].

This study is connected to the United Nations Sustainable Development Goals, particularly SDG 9, SDG 11, and SDG 16, which emphasize innovation, sustainable urban development, and strong institutional governance. By introducing a governance model for blockchain-based IoT ecosystems, this research contributes to the discussion on how digital infrastructures can be designed to be both secure and reliable while remaining practically deployable. The use of decentralized governance mechanisms and smart contracts helps clarify responsibility among participating entities and supports more consistent data management practices. As a result, the proposed approach has the potential to reduce risks related to data misuse and governance gaps, while also supporting the development of secure urban services and smart infrastructure. This highlights the importance of governance as a practical foundation for sustainable and inclusive technological development rather than a purely technical concern [15].

2. LITERATURE REVIEW

2.1. The Concept of the IoT

The IoT is a concept in which various physical devices are interconnected through the internet and can exchange information automatically without direct human intervention. Each device from sensors, cameras, and vehicles to household appliances has a unique Digital Identity (DI) and the capability to communicate and coordinate with other devices [16]. In its implementation, IoT technology has been widely utilized across various sectors such as smart farming, smart transportation, energy management, and digital healthcare services. However, the increasing number of interconnected devices has also introduced new challenges, particularly in terms of information security, privacy protection, and system reliability, since most current IoT infrastructures still rely on a centralized cloud-based architecture [17].

2.2. The Basic Concept of Blockchain Technology

Blockchain is a distributed and decentralized data storage and recording technology in which every transaction or piece of information is stored in interconnected data blocks. Each block contains the hash of the previous block, forming a chain of data that is difficult to modify without the consensus of all nodes in the network [18, 19]. The main advantages of blockchain technology include a high level of transparency, system reliability, strong data integrity, and the creation of a trustless environment that operates without a central authority. Initially, this technology was introduced through its use in cryptocurrencies such as Bitcoin, but it has since evolved and been applied across various fields, including supply chain management (logistics), financial services, digital governance, and the IoT. With the implementation of blockchain, data exchange and verification can be conducted more securely and efficiently, eliminating the need for third-party intermediaries since validation is performed collectively by all network participants [20].

2.3. Integration of Blockchain in IoT

The integration of blockchain technology into IoT emerges as a solution to various limitations found in conventional IoT systems. Through the implementation of blockchain, the security, privacy, and reliability of data generated by IoT devices can be significantly enhanced. In this architecture, every transaction or data exchange performed by IoT devices is permanently recorded on the blockchain ledger, making the information immutable and easily traceable to its origin [21]. In addition, the use of smart contracts automated programs that run on the blockchain network enables IoT devices to operate and interact autonomously without human intervention. For example, a temperature sensor in a storage room can transmit data to the blockchain system, which then automatically executes a digital contract to activate a cooling system if the temperature exceeds a predefined threshold [22]. With this integration, blockchain serves not only as a data security layer but also as an automated coordination mechanism that enables efficient collaboration among devices within large and complex IoT networks [23].

2.4. Existing Governance Models

Governance in the blockchain-IoT ecosystem plays a crucial role in regulating decision-making processes, determining access rights, and ensuring transparency and compliance within a decentralized network. Through effective governance, the system can operate efficiently and fairly for all participating entities [24, 25].

Several types of governance models that have been previously introduced include:

2.4.1. Centralized Governance Model

In this model, decision-making processes and system oversight are controlled by a single central entity, such as an organization or service provider. This approach offers advantages in terms of ease of control and faster decision-making. However, it does not fully reflect the decentralization principles that characterize blockchain technology.

2.4.2. Distributed Governance Model

In this model, responsibilities and oversight functions are shared among multiple nodes or stakeholders within the network. This system is more inclusive and flexible but requires strong coordination among participants to ensure that decision-making processes remain consistent and efficient.

2.4.3. Hybrid (Semi-Decentralized)

This model combines central control with user participation in the governance process. Such an approach is commonly used in enterprise blockchain systems, as it is considered more practical to implement within business environments that still require a clearly defined organizational structure.

Although various governance models have been proposed, the main challenge still lies in achieving a balance between security, operational efficiency, and decentralization principles, especially when applied to large-scale and complex IoT networks. This challenge emphasizes the need for coordination among multiple actors, rule-setting mechanisms, and accountability structures in complex socio-technical systems [26, 27]. In addition, the concept of explains how trust can be established through cryptographic mechanisms, consensus protocols, and transparent ledgers rather than centralized authorities. These perspectives provide the theoretical rationale for structuring governance into device-level control, smart contract-based automation, and consortium-level oversight in the proposed multilayer model [28, 29].

From a theoretical perspective, this study is grounded in governance theory, which emphasizes the coordination of multiple actors, rule-setting mechanisms, and accountability structures in complex socio-technical systems. In addition, the concept of distributed trust in blockchain networks highlights how trust can be established through cryptographic mechanisms, consensus protocols, and transparent ledgers rather than centralized authorities. By integrating these perspectives, this research positions blockchain-enabled IoT governance as a form of decentralized socio-technical governance, where technical infrastructures and organizational arrangements jointly shape system reliability, security, and legitimacy [30, 31, 32].

3. RESEARCH METHOD

3.1. Type of Research

This research employs a qualitative approach with a descriptive-conceptual nature. The study is structured into three main stages that include a systematic literature review to identify governance, security, and architectural challenges in blockchain and IoT systems, a comparative analysis of existing governance models to examine their strengths and limitations, and a conceptual synthesis to formulate the proposed multilayer governance framework. This approach enables an in-depth understanding of governance systems in the integration between blockchain and IoT technologies [33]. The qualitative method is used to analyze various literature sources and previous research findings to formulate a governance model relevant to the blockchain-IoT ecosystem. In this study, peer-reviewed journal articles, conference proceedings, and authoritative survey papers published within the last decade were systematically selected based on their relevance to blockchain governance, IoT architectures, security mechanisms, and smart contract applications [34]. To ensure rigor in the qualitative process, this study adopts a structured literature-based design in which sources are systematically identified, screened, and categorized based on their relevance to blockchain governance, IoT architectures, security mechanisms, and smart contract applications [35].

3.2. Analytical Approach Used

The analytical approach applied in this research utilizes descriptive-comparative and conceptual analysis, which are organized into a sequential flow consisting of literature analysis, model comparison, and conceptual model development to ensure methodological clarity and logical consistency [36, 37].

3.3. Literature and Previous Research Analysis

The initial stage involves reviewing various literature sources and previous studies related to blockchain governance, IoT security aspects, and the integration between the two technologies. The goal of this stage is to gain a comprehensive understanding of existing governance model implementations and to identify the limitations that still persist.

3.4. Comparative Analysis of Existing Models

The next step involves comparing various governance models that have been implemented in both blockchain systems and conventional IoT systems. Through this comparative analysis, the study aims to identify the strengths, weaknesses, and potential adaptations of each model that can be integrated within the blockchain-IoT context.

3.5. Conceptual Analysis and Model Development

Based on the results of the literature review and comparative analysis, a conceptual synthesis is conducted to develop a new governance model that balances decentralization, efficiency, and security aspects within the blockchain-IoT ecosystem [38]. The resulting model is then subjected to conceptual validation by assessing its internal consistency, alignment with established governance theory and best practices reported in prior studies, and its logical feasibility for application in representative IoT scenarios.

3.6. Steps in Developing a Governance Model

To clarify the sequence of methodological stages used in this study, the development process is organized into several structured steps that guide the formulation of the proposed governance model [39]. These steps encompass problem identification, literature analysis, comparative evaluation, conceptual formulation, and validation processes. The detailed description of each stage, including the activities performed and their corresponding objectives.

Table 2. Steps in Developing a Governance Model

Stage	Activities Conducted	Main Objective
Problem Identification.	Identify governance issues in blockchain IoT integration of blockchain and IoT, such as security, coordination, and decision-making.	Determine the research focus.
Literature Review and Existing Models.	Examine various governance models discussed in blockchain and IoT literature.	Understand the fundamental concepts and weaknesses of previous models.
Comparative Analysis.	Compare existing governance models from previous studies.	Identify gaps and potential areas for improvement.
Conceptual Model Conceptual Formulation.	Develop an initial design of a governance model adapted to the characteristics of blockchain-IoT systems.	Develop a new theoretical framework a new theoretical framework.
Conceptual Validation.	Conduct logical verification of the proposed model based on relevant theories and best practices.	Ensure the conceptual feasibility of the model.
Recommendation Development.	Formulate implications and recommendations for implementing the proposed governance model in practice.	Provide guidance for developers and stakeholders.

Table 2 presents a structured and sequential overview of the stages involved in developing a comprehensive governance model for the blockchain IoT system, beginning with systematic problem identification supported by an extensive review of relevant literature to capture existing challenges, technological gaps, and

governance limitations in current implementations. This stage is followed by a comparative evaluation of established governance models to examine their respective strengths, weaknesses, and contextual applicability across key dimensions such as security mechanisms, operational efficiency, scalability, and levels of decentralization [40]. The insights obtained from this evaluation form the conceptual foundation for constructing a governance model that emphasizes a balanced integration of security, efficiency, and decentralization within the blockchain IoT ecosystem. The proposed model is subsequently subjected to theoretical validation by aligning it with established principles and frameworks in distributed systems, information security, and digital governance. Finally, the process culminates in the formulation of practical and actionable recommendations intended to support researchers and system developers in designing and implementing robust, scalable, and sustainable blockchain IoT governance architectures [41, 42, 43].

To provide a clearer understanding of the methodological flow employed in this study, the process of developing the governance model is systematically structured into three interrelated and sequential stages. The first stage involves a comprehensive literature review that serves as the conceptual foundation by synthesizing existing theories, frameworks, and empirical findings related to blockchain, IoT, and governance mechanisms [44]. Building upon the insights derived from these stages, the final stage focuses on the formulation of the proposed governance model, which integrates theoretical insights with analytical findings to address identified gaps. This structured sequence is visually illustrated in Figure 1 through a methodological pyramid that highlights the hierarchical and progressive relationship among the three stages [45].

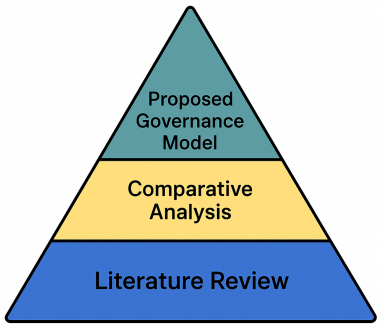

Figure 1. Pyramid model of the research stages

As shown in Figure 1, the model development process begins with an extensive literature review forming the foundational layer. This is followed by a comparative analysis that assesses the strengths, limitations, and applicability of various governance models identified in previous studies. The process culminates in the formulation of the proposed governance model, representing a synthesized outcome derived from conceptual grounding and critical evaluation. The tiered structure in the figure highlights that the final model is produced through a systematic, evidence-based progression rather than a single isolated step [46].

4. RESULT AND DISCUSSION

4.1. Device Governance Layer

This layer serves as the fundamental foundation for managing IoT devices. Registration, authentication, and data verification are carried out through a DI system that utilizes blockchain technology. Each IoT device is assigned a Unique Digital (UD), which is verified within a decentralized network, ensuring that only legitimate and authorized devices can send or receive information. This approach significantly reduces the risks of device identity spoofing and data tampering, which are common vulnerabilities in conventional IoT systems. Consequently, this layer enhances trust and data integrity throughout the entire IoT ecosystem [47, 48].

This section elaborates the proposed multilayer governance model for blockchain-integrated IoT ecosystems as a conceptual foundation to address key challenges of decentralization, security, and coordination, by structuring governance into device governance, smart contract automation, and consortium-level oversight in a coherent and logical manner [49]. The formulation of these governance layers is derived from a systematic

qualitative analysis of prior studies on blockchain governance, IoT architectures, and security frameworks, combined with a comparative evaluation of centralized, distributed, and hybrid governance models discussed in the literature. Through this synthesis, recurring issues related to device identity management, automation of trust, and stakeholder accountability were identified and mapped into the three proposed layers. The model integrates technical automation with organizational and human oversight by structuring governance into three interrelated layers: Device Governance, Smart Contract, and Consortium Governance. Unlike conventional single-layer approaches, this multilayer structure aligns device-level security, smart contract-based automation, and consortium-level policy control into a coherent framework. This conceptual contribution is expected to serve as a reference for future empirical studies and practical implementations in diverse application domains such as smart cities, healthcare, and industrial IoT.

4.2. Smart Contract Layer

The Smart Contract Layer plays a key role in managing automation within a blockchain-based IoT ecosystem. At this layer, governance rules such as device access rights, data sharing procedures, and transaction mechanisms are translated into smart contracts that run automatically on the blockchain. Once predefined conditions are fulfilled, the contracts execute without manual intervention, making system operations more efficient and consistent [50]. This approach not only reduces operational complexity and human error but also strengthens trust, as all actions are transparently recorded and can be verified. As a result, the Smart Contract Layer supports secure collaboration and smooth interaction across diverse IoT platforms and service providers.

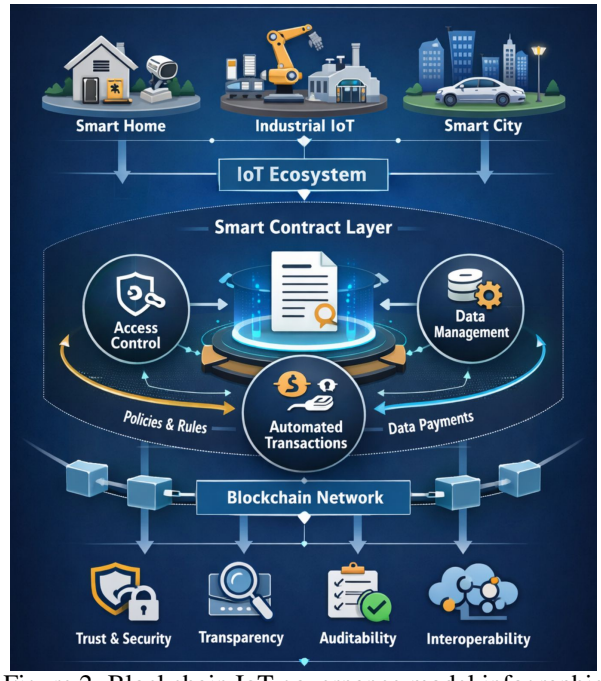

Figure 2. Blockchain IoT governance model infographic

Figure 2 illustrates a layered governance architecture for a blockchain-integrated IoT ecosystem. At the top level, the IoT ecosystem is represented by three major domains Smart Home, Industrial IoT, and Smart City which reflect the diversity of connected environments and devices. These domains are unified within a single IoT ecosystem that generates data and operational events. The indicates that interactions and data exchanges from IoT devices are not handled directly but are routed through a governance mechanism to ensure coordinated control, consistency, and policy enforcement across heterogeneous IoT environments. All executed actions are subsequently recorded and validated within the Blockchain Network at the lower layer, which provides essential governance properties, including trust and security, transparency, auditability, and interoperability. Through this layered structure, the figure emphasizes the role of smart contracts as digital trust mechanisms that eliminate reliance on intermediaries while ensuring integrity, accountability, and seamless integration across diverse IoT platforms.

4.3. Consortium Governance Layer

This layer occupies the highest level within the governance architecture and serves as a bridge between automated technical systems and human oversight. The Consortium Governance Layer involves multiple stakeholders such as developers, enterprises, regulators, and industry partners who collaboratively manage policies, system updates, conflict resolution, and ensure compliance with applicable norms and regulations. Through this approach, the strategic and normative elements of the blockchain-IoT system can be governed collectively. For instance, in situations where protocol revisions or dispute resolutions between nodes are required, decisions can be made collaboratively by consortium members through voting mechanisms or mutual agreements. This layer also plays a crucial role in aligning the technical automation enabled by smart contracts with human accountability. In this way, the system not only emphasizes technological productivity and security but also incorporates ethical, legal, and social considerations in its implementation.

5. MANAGERIAL IMPLICATIONS

The integration of Blockchain and IoT requires strengthened technology governance through a multilayer framework consisting of the Device Governance Layer, Smart Contract Layer, and Consortium Governance Layer. This structure ensures effective inter-device coordination, operational transparency, and human accountability in system oversight. To support practical implementation, organizations can adopt the ISO/IEC 30141 IoT Reference Architecture as a guideline to map device management, data flows, and governance functions into the proposed multilayer model, ensuring architectural consistency and interoperability. In addition, blockchain significantly enhances data security and risk management by replacing centralized architectures with decentralized and distributed ledgers, reducing vulnerabilities to cyberattacks and data manipulation. From a managerial perspective, organizations are encouraged to implement digital identities for IoT devices and utilize smart contracts as automated authentication and control mechanisms to create a secure, transparent, and auditable operational environment.

Furthermore, smart contracts play a crucial role in improving operational efficiency and process automation by enabling faster, more accurate execution of governance rules and transactions without manual intervention. This shift requires organizations to prepare skilled human resources in blockchain technology, cybersecurity, and cyber law to supervise and update automated systems. As an actionable strategy, practitioners are encouraged to align device authentication, access control, and incident response mechanisms with the NIST IoT Cybersecurity Framework, particularly in implementing risk identification, protection, detection, response, and recovery functions within smart contract logic and device governance policies. Through the Consortium Governance Layer, collaboration among developers, industry players, and regulators becomes essential to ensure legal compliance, interoperability, and ethical use of technology. Strategically, this governance model supports sustainable innovation by promoting decentralization and interoperability, enhancing organizational competitiveness, resilience, and the long-term sustainability of the digital ecosystem

6. CONCLUSION

This study presents a governance model that integrates blockchain technology into the IoT ecosystem to enable more secure, transparent, and decentralized coordination among devices and stakeholders. The proposed model addresses key governance challenges by strengthening data security, enhancing system reliability, and ensuring accountability in the management of distributed IoT networks. By leveraging blockchain's decentralized architecture and immutable ledger, the model reduces reliance on centralized control while fostering trust and data integrity across interconnected entities.

Beyond technical considerations of security and decentralization, this study contributes by offering a structured and conceptually grounded governance framework for blockchain-enabled IoT systems. The proposed multilayer model clarifies roles, responsibilities, and control mechanisms among stakeholders, providing a coherent theoretical foundation for understanding governance dynamics in complex IoT environments. This contribution positions governance as a critical factor in supporting sustainable, scalable, and trustworthy IoT ecosystems.

The findings of this study also highlight directions for future research and practical implementation. The proposed governance model may be extended and empirically validated through case studies, simulations, or pilot deployments in various IoT domains such as smart cities, healthcare, energy, and industrial systems.

Further investigation into governance effectiveness, system performance, and stakeholder adoption will support the refinement and real-world applicability of blockchain–IoT governance frameworks.

7. DECLARATIONS

7.1. About Authors

Rizki Indrawan (RI) https://orcid.org/0009-0004-8063-5301
Arista Ratih (AR) https://orcid.org/0009-0007-4519-5277
Harry Agustian (HA) https://orcid.org/0009-0006-8012-2260
Richard Evans (RE) https://orcid.org/0009-0007-7280-8323

7.2. Author Contributions

Conceptualization: RI, AR, HA and RE; Methodology: RI; Software: AR; Validation: HA and RE; Formal Analysis: RI and AR; Investigation: HA; Resources: RE; Data Curation: RI; Writing Original Draft Preparation: AR and HA; Writing Review and Editing: RE; Visualization: RI; All authors, RI, AR, HA, and RE 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] S. R. S. Vadivel, V. Karthikeyan, K. Gopalakrishnan *et al.*, "Introduction to the internet of things (iot)," in *Internet of Things Security*. Elsevier, 2026, pp. 3–31.
[2] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, vol. 24, no. 2, pp. 393–414, 2022.
[3] R. Faza, R. A. Darmawan, and D. T. Setiamanah, "Evaluation of rebar waste rate calculation model utilizing bim function: High rise building case study," *Aptisi Transactions on Technopreneurship*, vol. 5, no. 2, pp. 128–135, 2023.
[4] A. Razmjoo, A. Gandomi, M. Mahlooji, D. Astiaso Garcia, S. Mirjalili, A. Rezvani, and S. Memon, "An investigation of the policies and crucial sectors of smart cities based on iot application," *Applied Sciences*, vol. 12, no. 5, p. 2672, 2022.
[5] F. Nurdianingsih, W. N. Wahid, and J. Parker, "Comparative analysis of cloud storage architectures for scalability and security," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 182–193, 2026.
[6] I. Ullah and P. J. Havinga, "Governance of a blockchain-enabled iot ecosystem: A variable geometry approach," *Sensors*, vol. 23, no. 22, p. 9031, 2023.
[7] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11 475–11 490, 2022.
[8] J. Bojič Burgos and M. Pustišek, "Decentralized iot data authentication with signature aggregation," *Sensors*, vol. 24, no. 3, p. 1037, 2024.
[9] A. Kanivia, H. Hilda, A. Adiwijaya, M. F. Fazri, S. Maulana, and M. Hardini, "The impact of information technology support on the use of e-learning systems at university," *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 122–132, 2024.

[10] R. Supriati, N. Lutfiani, D. Apriani, A. Rizky *et al.*, "Utilizing the potential of blockchain technology for leading education 4.0," in *2022 International Conference on Science and Technology (ICOSTECH)*. IEEE, 2022, pp. 01–08.

[11] G. Lazaroiu, A. Androniceanu, I. Grecu, G. Grecu, and O. Neguriţă, "Artificial intelligence-based decision-making algorithms, internet of things sensing networks, and sustainable cyber-physical management systems in big data-driven cognitive manufacturing," *Oeconomia Copernicana*, vol. 13, no. 4, pp. 1047–1080, 2022.

[12] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of iot: A comprehensive review of iot applications and future prospects," *Sensors*, vol. 23, no. 16, p. 7194, 2023.

[13] P. K. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, "Blockchain technology and its types: A short review," *International Journal of Applied Science and Engineering*, vol. 9, no. 2, pp. 189–200, 2021.

[14] D. Apriani, V. T. Devana, A. P. Sagala, P. A. Sunarya, U. Rahardja, and E. P. Harahap, "Security using blockchain-based otp with the concept of iot publish/subscribe," in *AIP Conference Proceedings*, vol. 2808, no. 1. AIP Publishing, 2023.

[15] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: An overview," *PeerJ Computer Science*, vol. 9, p. e1705, 2023.

[16] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54 478–54 497, 2021.

[17] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating iot and blockchain technologies," *Heliyon*, vol. 10, no. 19, 2024.

[18] H. Altamimi, Q. Liu, and B. Jimenez, "Not too much, not too little: Centralization, decentralization, and organizational change," *Journal of Public Administration Research and Theory*, vol. 33, no. 1, pp. 170–185, 2023.

[19] N. Lutfiani, D. Apriani, E. A. Nabila, and H. L. Juniar, "Academic certificate fraud detection system framework using blockchain technology," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 55–64, 2022.

[20] B. Anthony Jnr, "Toward a collaborative governance model for distributed ledger technology adoption in organizations," *Environment Systems and Decisions*, vol. 42, no. 2, pp. 276–294, 2022.

[21] Y. Formery, L. Mendiboure, J. Villain, V. Deniau, and C. Gransart, "A framework to design efficient blockchain-based decentralized federated learning architectures," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 705–723, 2024.

[22] U. Khalil, O. A. Malik, M. Uddin, and C.-L. Chen, "A comparative analysis on blockchain versus centralized authentication architectures for iot-enabled smart devices in smart cities," *Sensors*, vol. 22, no. 14, p. 5168, 2022.

[23] R. M. Devi, M. Sangeetha, R. Venkatesan, L. Balasubramanian, and P. Keerthika, "Enhancing decentralized privacy through integration of blockchain with iot for healthcare applications," *Blockchain Technology for the Engineering and Service Sectors*, pp. 107–131, 2026.

[24] F. A. Alaba, "Iot architecture layers," in *Internet of Things: A Case Study in Africa*. Springer Nature Switzerland, 2024, pp. 65–85.

[25] W. Usino, D. A. R. Kusumawardhani, T. Ramadhan, A. Pratiangga, and O. Qurotulain, "Big data analytics: Transforming business intelligence and decision making," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 154–163, 2024.

[26] A. Asheralieva, "Blockchain-enabled autonomous iot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 2890–2902, 2022.

[27] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.

[28] R. Sheeba, H. Alsolai, R. Allafi, K. Nithya, M. A. Arasi, B. Karthikeyan, D. Sudarvizhi, and S. Vivek, "A comprehensive iot and blockchain-integrated framework for autonomous water management in sustainable urban ecosystems," *Sustainable Computing: Informatics and Systems*, p. 101171, 2025.

[29] P. Wells, G. Probert, D. Marke, and C. Konopka, "Position paper on applications of smart contracts and blockchain technology," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 48–53, 2023.

[30] W. Huang, Y. Han, Q. Gu, X. Han, and T. Gao, "Smart blockchain-powered natural resource asset management and ecological governance countermeasures," *Heliyon*, vol. 11, no. 2, 2025.

[31] C. Chakilam, P. K. Kumar, A. S. Nafais, M. M. Sampoornam, A. Balaram, and G. Swarnalakshmi, "Decentralized blockchain integrated ecosystems for equitable civic engagement and transparent digital policy

implementation in smart cities," in *International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 2024)*. Atlantis Press, 2025, pp. 355–366.

[32] F. Septiyana, M. S. Shihab, H. Kusumah, D. Apriliasari *et al.*, "Analysis of the effect of product quality, price perception and social value on purchase decisions for lampung tapis fabrics," *APTISI Transactions on Management*, vol. 7, no. 1, pp. 54–59, 2023.

[33] J. Gamboa-Cruzado, V. Pineda-Delacruz, H. Salcedo-Mera, C. Alzamora Rivero, J. Coveñas Lalupu, and M. Narro-Andrade, "Blockchain and data management security for sustainable digital ecosystems: A systematic literature review," *Sustainability*, vol. 18, no. 1, p. 185, 2025.

[34] G. Mustafa, W. Rafiq, N. Jhamat, Z. Arshad, and F. A. Rana, "Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations," *International Journal of Law and Management*, vol. 67, no. 1, pp. 37–55, 2025.

[35] A. Cholke, V. Mandhare, and P. Vikhe, "A review of security and information control in blockchain-integrated iot applications," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. IEEE, 2024, pp. 1–6.

[36] P. Ranjitha, "Security challenges in iot-blockchain integrated ecosystems," *International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)*, vol. 1, no. 4, pp. 36–44, 2025.

[37] S. Watini, L. Magdalena, T. W. Wirjawan, A. Gunawan, D. Julianingsih, and N. Ivanov, "Social media as a tool for transforming childhood learning mechanisms in edupreneurship," *Aptisi Transactions on Technopreneurship*, vol. 7, no. 1, pp. 109–119, 2025.

[38] K. Patel *et al.*, "Iot data governance frameworks," *Journal of Information and Data Management*, vol. 13, no. 1, pp. 74–95, 2022.

[39] K. Swathi, P. Durga, K. V. Prasad, A. K. Chaitanya, K. Santhi, P. Vidyullatha, and S. V. A. Rao, "Secure blockchain integrated deep learning framework for federated risk-adaptive and privacy-preserving iot edge intelligence sets," *Scientific Reports*, vol. 15, no. 1, p. 41133, 2025.

[40] L. Jimenez-Castillo, J. Sarkis, S. Saberi, and T. Yao, "Blockchain-based governance implications for ecologically sustainable supply chain management," *Journal of Enterprise Information Management*, vol. 37, no. 1, pp. 76–99, 2024.

[41] B. Khayer, S. Mirzaei, H. Alavizadeh, and A. Salehi Shahraki, "Blockchain for secure iot: A review of identity management, access control, and trust mechanisms," *IoT*, vol. 6, no. 4, p. 65, 2025.

[42] M. R. Anwar and L. D. Sakti, "Integrating artificial intelligence and environmental science for sustainable urban planning," *IAIC Transactions on Sustainable Digital Innovation*, vol. 5, no. 2, pp. 179–191, 2024.

[43] P. Krishnan, K. Jain, S. R. Poojara, S. N. Srirama, T. Pandey, and R. Buyya, "esim and blockchain integrated secure zero-touch provisioning for autonomous cellular-iots in 5g networks," *Computer Communications*, vol. 216, pp. 324–345, 2024.

[44] A. S. Vindhya, V. S. Kumari, L. Karthikeyan, D. Vinoth, and M. Agoramoorthy, "A novel blockchain-integrated iot framework for secure and efficient vehicle-to-infrastructure communication in smart transportation," *Peer-to-Peer Networking and Applications*, vol. 18, no. 6, p. 324, 2025.

[45] S. Sutradhar, R. Bose, S. Majumder, A. A. Khan, S. Roy, F. Ullah, and D. Prashar, "Mediguard: A survey on security attacks in blockchain-iot ecosystems for e-healthcare applications." *Computers, Materials & Continua*, vol. 83, no. 3, 2025.

[46] A. CR, A. K. Pani, and P. Kumar, "Blockchain-enabled smart contracts and the internet of things: Advancing the research agenda through a narrative review," *Multimedia Tools and Applications*, vol. 84, no. 8, pp. 5097–5147, 2025.

[47] Ministry of Communication and Information Technology of the Republic of Indonesia, "National digital transformation policy for artificial intelligence and data governance," Official government publication, 2023, policy document retrieved from Indonesian government domain (go.id).

[48] M. M. Hossain, M. A. Rahman, S. Chaki, H. Ahmed, A. Haque, I. Tamanna, S. Lima, J. F. Most, and M. S. Rahman, "Smart-agri: A smart agricultural management with iot-ml-blockchain integrated framework," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 7, 2023.

[49] A. C. Careja and N. Tapus, "Digital identity using blockchain technology," *Procedia Computer Science*, vol. 221, pp. 1074–1082, 2023.

[50] C. S. Babu and G. Gokul, "Smart contracts in ai-driven decentralized finance: Navigating emerging technologies and market dynamics," *Emerging Trends and Innovations in Financial Services: A Futurology Perspective*, pp. 191–234, 2026.