Blockchain Frontier Technology (BFRONT)
Vol. 6, No. 1, July 2026, pp. 13∼24
E-ISSN: 2808-0009 | P-ISSN: 2808-0831, DOI: 10.34306

Blockchain Integration for Secure Data Provenance and Interoperable Database Management

Terra Saptina Maulani[1], Dwi Cahyono[2], Yansa Sendi Fadillah[3*], Maulidya Reva Aprianti[4], John Edwards[5]
[1]Faculty of Economic, Parahyangan Catholic University, Indonesia
[2]Faculty of Economic and Business, University of Muhammadiyah Jember, Indonesia
[3,4]Faculty of Science and Technology, University of Raharja, Indonesia
[4]Department of Information Technology, Pandawan Incorporation, New Zealand
[1]19011901001@student.unpar.ac.id, [2]dwicahyono@unmuhjember.ac.id, [3]yansa.sendi@raharja.info, [4]maulidya@raharja.info
[5]no.rangi3@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission, 24-12-2025
Revised, 18-02-2026
Accepted, 09-03-2026
Published, 26-03-2026

Keywords:

Blockchain Integration
Secure Data Provenance
Database Management
Hybrid Architecture
Data Integrity

ABSTRACT

The rapid advancement of digital technologies has led to a significant increase in data volume and complexity, while traditional database systems continue to face challenges in ensuring data security, integrity, transparency, and interoperability across platforms, resulting in higher risks of data tampering, limited audit trails, and the formation of data silos. **This study aims** to examine and develop a blockchain integration model with conventional database systems to strengthen secure data provenance and enhance interoperability among heterogeneous databases. **This research proposes** a hybrid architecture that combines on data recording using a permissioned blockchain with off data storage through Relational Database Management System (RDBMS) or Not Only SQL (NoSQL) databases, where blockchain functions as a trust layer that records data hashes, metadata, and immutable change histories, while system evaluation is conducted through security testing, data integrity assessment, auditability analysis, latency measurement, throughput evaluation, data consistency analysis, and cross-platform interoperability testing. **The experimental results** demonstrate that blockchain integration significantly improves data security and traceability by providing transparent and tamper-resistant audit trails, while enabling secure and consistent data exchange across systems through integration modules and API gateways, despite introducing additional performance overhead compared to conventional database systems. **This study concludes** that integrating blockchain with conventional database systems is an effective approach for ensuring secure data provenance and interoperable database management, offering a balanced trade-off between security, transparency, and system efficiency, and presenting strong potential for further development in large-scale distributed data environments.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.34306/bfront.v6i1.1025
This is an open-access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

The rapid advancement of digital technologies has led to a significant increase in data volume and complexity. However, traditional database systems still face numerous challenges in maintaining data security, authenticity, and consistency across platforms [1]. One of the primary issues is the risk of data manipulation (data tampering), which can occur both internally and externally, particularly when access control mechanisms and data change logging are not properly designed. In addition, the lack of transparency in data management processes makes it difficult to trace data modification histories, thereby complicating audit and verification activities [2]. Another challenge arises from the formation of data silos, where data is distributed across multiple disconnected systems, hindering interoperability and information exchange among organizations or platforms.

These interoperability limitations directly impact operational efficiency and reduce organizations' ability to perform comprehensive data integration. Slow synchronization processes, differences in data structure standards, and the absence of secure data exchange mechanisms further exacerbate these issues. Consequently, a new approach is required that can provide secure data provenance while simultaneously supporting more effective cross-database integration [3]. Blockchain has emerged as a potential solution to address these challenges. With characteristics such as decentralization, immutability, consensus mechanisms, and automated execution through smart contracts, blockchain can ensure that every data transaction is recorded transparently, cannot be altered, and can be audited at any time [4]. Moreover, integrating blockchain with conventional database systems enables the creation of an interoperable data ecosystem without the need to replace existing systems, thereby enhancing both efficiency and security.

Although numerous studies have explored the use of blockchain for data security and interoperability, several research gaps remain insufficiently addressed. Some studies have not comprehensively examined how blockchain integration can be implemented within hybrid architectures involving both on-chain and off-chain data [5]. Furthermore, performance evaluations related to latency, throughput, and data consistency in distributed environments are still limited. This indicates the need for further research focusing on the implementation of integrative architectures and in-depth performance evaluation.

Based on the above background, this study is formulated to address the following key research questions:

- How can blockchain be utilized to strengthen secure and transparent data provenance?
- How can blockchain integration enhance interoperability among heterogeneous database systems?
- What type of system architecture is effective for integrating blockchain with conventional database systems?
- How does the performance of the proposed hybrid system compare with that of traditional systems?

In addition to these system-level questions, this study also explores how the proposed architecture can be implemented in organizational contexts to support secure data governance, cross-institutional collaboration, and trusted digital service delivery [6]. This action-oriented perspective ensures that the proposed model is evaluated not only from a technical standpoint but also from its applicability in real-world operational environments [7]. Beyond technical evaluation, these research questions are positioned to examine how blockchain-integrated database architectures can influence organizational decision-making, governance practices, and cross-system collaboration in real operational environments. By framing the investigation in both technical and applied contexts, the study aims to generate actionable insights for practitioners and institutions seeking to implement secure and interoperable data infrastructures [8].

This study aims to develop a blockchain integration architecture model that enhances data security, ensures transparency of data histories, and enables interoperability among database systems. The scientific contributions of this research include the proposal of a novel architecture, the development of integration modules, and a comprehensive performance evaluation through a series of experiments and testing scenarios. This article is structured as follows, the first section reviews relevant literature, the second section describes the proposed methodology and system architecture, the third section presents the experimental results and discussion, and the final section outlines managerial implications, conclusions, and recommendations for future research.

In addition to its technical contributions, this study is also relevant to the achievement of the Sustainable Development Goals (SDGs), particularly SDGs 9 (Industry, Innovation, and Infrastructure) and SDGs

16 (Peace, Justice, and Strong Institutions). The integration of blockchain with database systems supports the development of reliable, secure, and innovative digital infrastructure by enhancing transparency, integrity, and reliability in data management [9]. The implementation of secure data provenance and database interoperability contributes to more accountable information governance, particularly in the public sector, finance, healthcare, and data-driven industries [10]. By providing transparent and auditable data recording mechanisms, this approach helps strengthen trust in digital information systems, promotes cross organizational collaboration, and supports sustainable, data-driven decision making in line with the principles of sustainable development outlined in the SDGs. This research also aligns with frontier and applied innovation perspectives by demonstrating how blockchain-integrated database architectures can be implemented in real organizational environments [11]. In practical contexts, the proposed model is applicable to sectors requiring high data integrity and cross-organizational collaboration, such as public administration, financial auditing, healthcare information systems, and digital supply chain management [12]. For example, in public sector governance, blockchain-based data provenance can enhance transparency in document management and regulatory reporting. In financial and audit institutions, immutable logging and verifiable data histories can strengthen compliance monitoring and fraud detection. Meanwhile, in healthcare and multi-institutional environments, interoperable database integration supported by blockchain can enable secure data sharing without compromising privacy or system autonomy [13].

In contrast to existing hybrid blockchain–database implementations that primarily focus on technical integration, this study introduces an applied architectural perspective that integrates blockchain as a governance-oriented trust layer, enabling cross-system auditability, decision-support transparency, and operational workflow alignment across organizational domains [14]. The proposed model further contributes by linking interoperability mechanisms with practical data governance strategies, thereby positioning the architecture as a scalable framework for interdisciplinary and real-world institutional deployment.

2. LITERATURE REVIEW

2.1. Data Provenance

Data provenance refers to information that describes the origin of data, the processes through which it is generated, and the history of changes that occur throughout the data lifecycle [15]. In modern database systems, data provenance plays a crucial role in ensuring data authenticity [16], integrity, and traceability, particularly in distributed environments and systems involving multiple users and cross-organizational data exchange.

The presence of reliable data provenance mechanisms supports audit, validation, and regulatory compliance processes. With clear provenance information, organizations can trace how data is generated and modified, thereby increasing trust in the quality of data used for decision-making. Without proper data history recording, data transparency and accountability become difficult to maintain [17]. However, the implementation of data provenance in traditional database systems still faces several challenges, such as difficulties in preserving the integrity of data modification histories, the risk of manipulation in centralized logging systems, and weak audit trail mechanisms [18]. These limitations highlight the need for solutions capable of recording every data change in a secure, transparent, and immutable manner to ensure consistent and reliable data provenance [19].

2.2. Interoperable Database Management

Interoperable database management refers to the ability of multiple database systems to exchange, access, and interpret data effectively. In distributed system environments, interoperability is a critical requirement, as data is often stored across different platforms with diverse technologies and data structures [20]. Data exchange standards such as APIs, JSON, and XML have been widely adopted to support communication among systems. Nevertheless, conventional database systems still face various challenges in achieving optimal interoperability. Differences in data schemas, storage models, and communication protocols complicate cross-platform integration [21]. In addition, security and access control aspects pose significant challenges, particularly when data must be shared across organizations with differing policies and infrastructure.

As a result of these limitations, many organizations continue to rely on isolated systems or data silos, which hinder operational efficiency and collaboration. This condition leads to delays in information exchange and reduces the quality of decision-making. Therefore, a database management approach is required that

can support interoperability in a secure, consistent, and sustainable manner [22]. Recent interdisciplinary studies in digital governance, information systems management, and enterprise data infrastructure highlight the importance of trusted data ecosystems that integrate security, interoperability, and auditability. Applied research in sectors such as finance, healthcare, and public administration demonstrates that hybrid blockchain architectures can support regulatory compliance, cross-organizational data sharing, and collaborative digital services [23]. By integrating insights from these applied domains, the proposed architecture is positioned not only as a technical solution but also as a practical framework for managing trusted data exchange and accountability in complex organizational environments [24].

2.3. Blockchain in Data Management

Blockchain is a distributed technology that offers key characteristics such as decentralization, immutability, consensus mechanisms, and smart contracts [25]. These characteristics make blockchain highly relevant for enhancing data security and reliability, particularly in ensuring the integrity and transparency of data modification histories [26]. In the context of data management, blockchain can serve as a trust layer that permanently records data transactions in an auditable manner. Numerous previous studies have demonstrated that blockchain adoption can preserve data integrity and support secure information exchange across systems and organizations. Through consensus mechanisms and distributed ledgers, blockchain reduces reliance on centralized authorities and mitigates the risk of data manipulation [27]. Furthermore, the use of smart contracts enables the automation of data validation and access control processes based on predefined rules [28].

Nevertheless, several research gaps remain insufficiently addressed. Performance evaluations of blockchain integration architectures with conventional database systems are still limited, particularly with respect to latency, throughput, and data consistency. In addition, blockchain-based interoperability standards have not been extensively investigated, and synchronization mechanisms between on-chain and off-chain data still require more optimized approaches [29]. These limitations highlight opportunities for further research in advancing blockchain integration with modern database systems. To provide a unifying theoretical lens, this study adopts a socio-technical and digital governance perspective in which blockchain functions as an institutional trust infrastructure that supports verifiable data provenance and interoperable information exchange across organizational boundaries [30]. Within this perspective, data provenance represents the traceability dimension of digital trust, interoperability reflects the coordination dimension across heterogeneous systems, and blockchain acts as the enabling infrastructure that operationalizes these dimensions through immutable logging and consensus-based validation [31]. This integrated lens links the conceptual discussion directly to the proposed system architecture and empirical evaluation, where security, traceability, interoperability, and performance metrics are examined as operational indicators of trusted digital infrastructure in organizational and cross-sector environments [32].

3. RESEARCH METHODS

3.1. Research Framework

This study adopts a conceptual model that integrates blockchain technology with conventional database systems to enhance data security and interoperability in distributed environments. The proposed framework is designed to address challenges related to data integrity, traceability, and cross-system coordination by combining the strengths of decentralized ledger technology and traditional data management systems.

Within this framework, blockchain functions as a trust layer that records metadata, data hashes, and data modification histories in an immutable and verifiable manner [33]. By anchoring cryptographic hashes of transactional data onto the blockchain, the system ensures that any unauthorized data alteration can be detected efficiently. This mechanism strengthens data provenance by providing transparent and tamper-resistant audit trails that can be independently verified across participating entities [34]. Meanwhile, conventional database systems are retained as the primary storage medium (off-chain) to preserve storage efficiency, scalability, and system performance. Sensitive or large-volume data remain stored in relational or NoSQL databases, while only essential verification elements are recorded on-chain. This hybrid configuration enables the system to balance security and operational efficiency, ensuring that blockchain integration enhances trust and interoperability without compromising performance [35].

The data management workflow is illustrated from the processes of data recording, validation, storage, to data synchronization across systems. Through this approach, the system is able to ensure that every

data modification can be traced and verified without compromising the flexibility and scalability of traditional database systems.

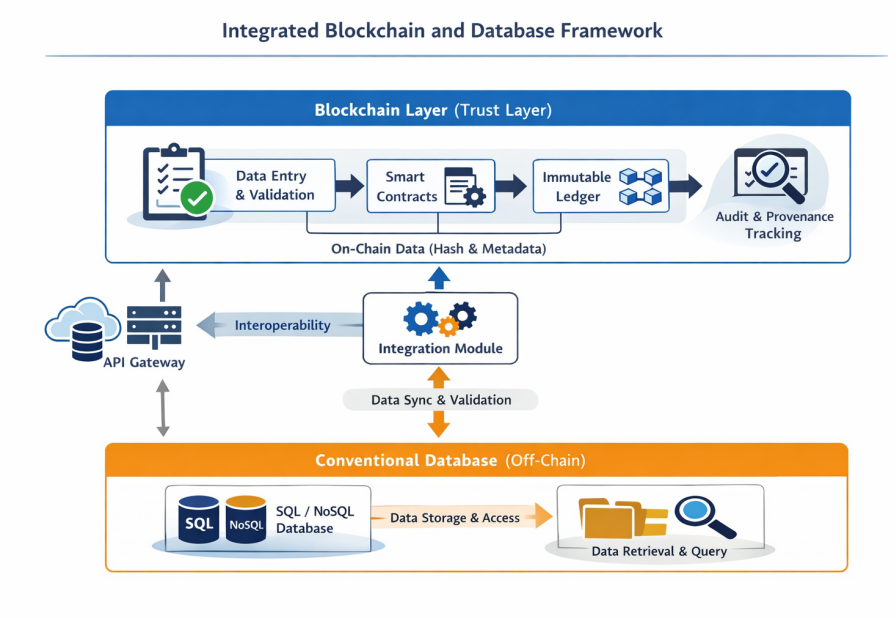


Figure 1. Conceptual Framework of Blockchain Integrated Database System

Figure 1 illustrates the conceptual model of integration between blockchain technology and conventional database systems. The model highlights the role of blockchain as a trust layer in ensuring data security and traceability, as well as the synchronization mechanism with off-chain databases to support system efficiency and interoperability.

3.2. System Architecture

The system architecture adopts a hybrid architecture that integrates a permissioned blockchain with conventional database systems. This approach is selected to ensure improved access control, a high level of security, and operational efficiency. To support interoperability across systems, an API gateway is employed as a standardized communication interface.

The main components of the system architecture include:

- On-chain data, which store data hashes, metadata, and provenance information as evidence of data integrity and authenticity.
- Off-chain databases, which store the primary data using RDBMS or NoSQL databases according to application requirements.
- Smart contracts, which govern the logic for data recording, transaction validation, and automated access control policies.
- Integration modules, which function as connectors between applications, the blockchain network, and database systems.
- Synchronization protocols, which ensure consistency and alignment between on-chain and off-chain data.

This architecture is designed to enable secure and transparent data exchange among heterogeneous systems without requiring significant modifications to existing infrastructure.

3.3. Experimental Setup

Experiments were conducted to evaluate the effectiveness and performance of the proposed hybrid blockchain–database architecture using multiple technology platforms [36]. A permissioned blockchain platform (e.g., Hyperledger Fabric) was implemented as the on-chain trust layer to record data hashes and provenance metadata, while RDBMS and NoSQL databases were used for off-chain storage to simulate heterogeneous environments [37]. IPFS supported distributed data referencing, and smart contracts managed transaction validation and access control [38]. The evaluation employed simulated and public datasets representing multi-system data modification and exchange scenarios under varying workload conditions (low, medium, and high). Key parameters measured included latency, throughput, scalability, data integrity, tamper detection, audit trail availability, cross-database compatibility, and synchronization effectiveness to ensure a structured and reproducible system assessment [39].

Table 1. Experimental Setup and Evaluation Parameters

Aspect	Description
Blockchain Platform	Hyperledger Fabric (permissioned blockchain)
Off-chain Storage	RDBMS and NoSQL databases
Distributed Storage	InterPlanetary File System (IPFS)
Smart Contract Function	Data recording, transaction validation, access control automation
Integration Mechanism	API Gateway and integration modules
Dataset Type	Simulated datasets and public datasets
Data Scenario	Data modification, data exchange, and multi-system transactions
Security Parameters	Data integrity, tamper detection, audit trail availability
Performance Parameters	Transaction latency, system throughput, scalability
Interoperability Metrics	Cross-database compatibility, data format consistency, synchronization effectiveness
Workload Scenarios	Low, medium, and high transaction loads

Table 1 summarizes the experimental setup and evaluation parameters used in this study. The table provides a structured overview of the technological platforms, system components, datasets, and evaluation metrics applied to assess the proposed blockchain-integrated database architecture. By presenting the experimental configuration in a concise format, helps clarify how data security, interoperability, and performance aspects are systematically evaluated under various workload conditions. This structured setup ensures that the experimental results are reproducible and that comparisons with conventional database systems can be conducted objectively and consistently [40]. The tools and platforms used include Hyperledger Fabric or Ethereum as the blockchain platform, IPFS as an additional distributed storage layer, and both RDBMS and NoSQL databases for off-chain data storage.

The datasets consist of simulated and public data representing transaction activities in multi-system environments. These datasets were designed to reflect various scenarios of data modification and data exchange [41]. This study also incorporates a domain-specific scenario to strengthen real-world applicability, particularly in the context of healthcare data exchange involving hospitals, laboratories, and insurance providers. In this scenario, the proposed hybrid blockchain–database architecture is used to record data provenance for patient records, validate inter-organizational transactions through smart contracts, and ensure consistent synchronization between on-chain metadata and off-chain clinical databases [42]. By simulating cross-institutional data sharing with strict access control and audit requirements [43], this additional case demonstrates how the architecture can support governance, regulatory compliance, and operational workflows in real organizational environments while maintaining data integrity, transparency, and interoperability [44].

The evaluation parameters cover data security aspects (integrity and tamper detection), transaction latency, system throughput, cross-database compatibility, and data consistency between on-chain and off-chain storage [45]. Experiments were carried out under various workload scenarios to assess the stability and reliability of the system.

4. RESULTS AND DISCUSSION

4.1. Impact on Secure Data Provenance

The test results indicate that blockchain integration provides a substantial improvement in the security and reliability of data provenance within the proposed architecture. Every data modification occurring in the off-chain database is systematically recorded in the form of cryptographic hashes and associated metadata on the on-chain ledger, creating a verifiable linkage between stored data and its historical record. Through the hash validation mechanism, any unauthorized alteration or inconsistency between off-chain data and on-chain records can be immediately detected, thereby ensuring continuous verification of data integrity. This mechanism strengthens trust in the accuracy, authenticity, and traceability of information across distributed systems, particularly in environments involving multiple users and cross-organizational data exchange.

Furthermore, the implementation of an immutable ledger proves highly effective in preventing data tampering and retrospective manipulation. Because records stored on the blockchain cannot be altered or deleted once validated through consensus, the system is capable of generating a complete, chronological, and transparent audit trail of all data-related activities. This capability is essential for audit processes, digital forensics investigations, and regulatory compliance requirements that demand precise traceability and accountability of data changes. By guaranteeing non-repudiation and verifiable transaction histories, blockchain operates as a robust trust layer within the data management system, reinforcing governance, transparency, and long-term data reliability.

4.2. Improvement in Interoperable Database Management

The interoperability evaluation shows that the proposed system is able to support cross-database integration more effectively than conventional systems [46]. By leveraging an API gateway and dedicated integration modules, the architecture enables structured and secure data exchange among heterogeneous databases without requiring modifications to the internal schemas or core logic of each system [47]. This design minimizes disruption to legacy infrastructures while establishing a standardized communication layer that facilitates controlled interoperability. The testing results demonstrate improved efficiency in data exchange and federated query processes, allowing coordinated management of data requests originating from multiple sources across distributed environments. Furthermore, system compatibility is strengthened through blockchain-based synchronization mechanisms that ensure data consistency, integrity, and traceability even when data is generated from diverse platforms and database technologies. By embedding verification and synchronization at the trust layer, the architecture reduces dependency on ad-hoc integration solutions, mitigates semantic and structural inconsistencies, and systematically addresses the long-standing issue of data silos. As a result, the proposed model not only enhances technical interoperability but also supports more reliable cross-system collaboration and governance-oriented data management.

4.3. Performance Evaluation

From a performance perspective, the results indicate that blockchain integration introduces additional latency in data recording compared to conventional systems. From an operational standpoint, these performance metrics provide decision-makers with measurable trade-offs between security assurance and processing speed. For instance, slightly higher latency may be acceptable in audit-critical environments where data integrity and traceability are prioritized, while throughput stability becomes more relevant for systems requiring continuous multi-departmental data synchronization [48]. These interpretations help translate technical metrics into actionable considerations for system adoption and governance planning. However, this latency remains within acceptable limits, particularly in permissioned blockchain architectures. The use of off-chain storage has also been shown to effectively reduce processing overhead and resource consumption on the blockchain [49]. Beyond technical performance, the proposed architecture introduces practical changes to organizational decision-making and governance processes. By ensuring that every data transaction is immutably recorded and verifiable across systems, decision-makers can rely on trusted data sources for operational planning, compliance reporting, and cross-departmental coordination. The availability of verifiable data provenance enables organizations to shift from reactive audit processes toward continuous, real-time data validation and governance. As a result, operational workflows such as data approval, reporting, and inter-system reconciliation can be automated and monitored transparently, reducing manual verification efforts and improving accountability across organizational units.

Figure 2 presents a comparative analysis between the blockchain-integrated system (hybrid system) and conventional database systems based on latency, throughput, and scalability parameters.

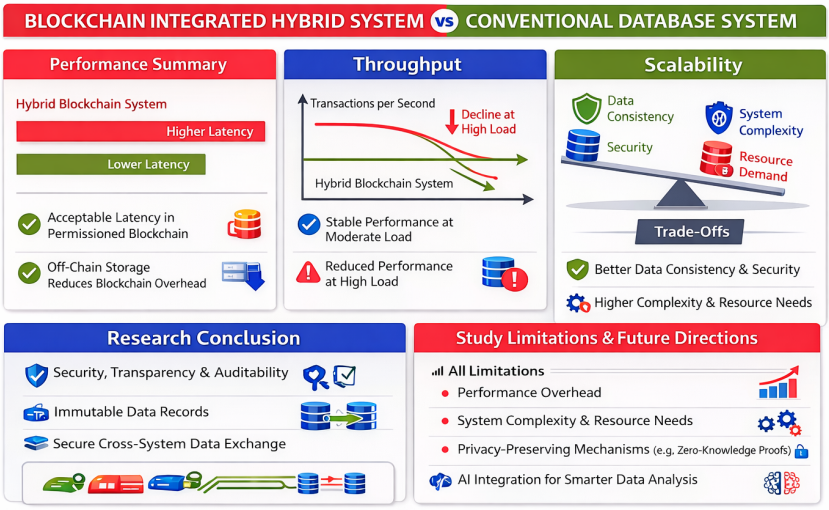


Figure 2. Performance Analysis of Hybrid Blockchain Based System versus Conventional Database System

The throughput analysis indicates that the hybrid system is capable of handling a stable transaction workload, although performance degrades when the number of transactions increases significantly. From an operational perspective, stable throughput implies that the system can reliably support routine organizational workloads such as periodic data synchronization, multi-system reporting, and collaborative data updates without significant disruption [50, 51]. This performance level is well suited for enterprise environments where consistency, traceability, and coordinated data exchange are prioritized over high-frequency real-time processing. In terms of scalability, the blockchain-integrated system better preserves data consistency and security than traditional systems, although it involves greater complexity and resource demands. Overall, it offers stronger security, transparency, and auditability, while conventional systems retain advantages in latency and implementation simplicity. To enhance practical relevance, the performance metrics are interpreted in terms of operational decision-making. Although blockchain introduces additional latency, it is acceptable in environments prioritizing compliance and auditability, while stable throughput supports secure enterprise synchronization. Overall, the results clarify trade-offs between performance efficiency, security assurance, and governance requirements in adopting blockchain-integrated databases.

Based on the research findings, integrating blockchain with conventional database systems significantly enhances secure data provenance and interoperability by positioning blockchain as a trust layer that ensures immutable, verifiable, and transparent transaction records, thereby strengthening data integrity, traceability, and accountability for operational, compliance, and strategic purposes. The hybrid approach enables secure cross-system data exchange across heterogeneous platforms without replacing existing infrastructures, combining on-chain verification and off-chain storage to maintain efficiency while improving transparency and coordination in governance-oriented environments. However, the architecture introduces performance overhead under high transaction volumes and increases system complexity, indicating the need for future research on scalability optimization, performance improvement, and the integration of privacy-preserving technologies such as zero-knowledge proofs and AI-driven data analysis.

5. MANAGERIAL IMPLICATIONS

The integration of blockchain with conventional database systems has important managerial implications, particularly for IT management and audit-oriented organizations. This hybrid architecture supports

cross-sector digital transformation by enabling secure, transparent, and interoperable data exchange among government institutions, enterprises, and data-driven industries. By functioning as a trust layer, blockchain enhances audit transparency, policy enforcement, and inter-organizational collaboration, while allowing organizations to modernize their digital infrastructure incrementally without disrupting legacy systems. As a result, organizations can improve trust in data quality and reliability for operational processes and strategic decision-making. Blockchain-based immutable records reduce data manipulation risks and enable continuous auditability, strengthening efficiency and accountability. Organizations should adopt a gradual hybrid implementation using permissioned blockchain and API integration, supported by clear security policies such as role-based access control, encryption standards, and recovery mechanisms to ensure sustainable governance. The architecture provides practical guidance for policy and IT governance by enabling verifiable data histories, regulatory compliance, standardized data sharing, and risk management, while fostering cross-sector collaboration to enhance decision-making, transparency, and digital governance.

6. CONCLUSION

This study investigates the integration of blockchain technology with conventional database systems as an approach to enhancing data provenance security and cross-database interoperability. This study contributes beyond existing hybrid blockchain implementations by positioning blockchain not only as a technical security layer but also as a governance-oriented trust infrastructure that supports transparent decision-making, cross-organizational data accountability, and operational workflow coordination. By linking interoperability mechanisms with applied data governance and institutional use scenarios, the proposed architecture provides a more practice-oriented framework that extends prior hybrid blockchain research. The results demonstrate that employing blockchain as a trust layer is effective in ensuring data integrity, providing transparent audit trails, and reliably detecting data modifications. The proposed hybrid architecture, which combines on-chain recording with off-chain data storage, is shown to preserve system efficiency while maintaining strong security and data traceability.

Furthermore, the evaluation results indicate that blockchain integration significantly improves interoperable database management. Through the use of integration modules and API gateways, the system is able to support secure, consistent, and controlled data exchange across heterogeneous platforms. Compared to conventional systems, the blockchain-based approach offers notable advantages in terms of transparency, auditability, and data reliability. However, the study also identifies increased system complexity and performance overhead as important considerations for practical implementation.

As future research directions, this study highlights opportunities for further development in blockchain scalability and performance optimization, particularly in environments with high transaction volumes. In addition, the integration of privacy-preserving mechanisms such as zero-knowledge proofs has the potential to protect sensitive data without reducing system transparency. Future studies may also explore the application of artificial intelligence for automated data provenance analysis and anomaly detection, enabling blockchain-based data management systems to become more intelligent, adaptive, and suitable for large-scale industrial deployment. Editorial refinements have been applied to enhance language precision, reduce redundancy, and ensure consistent terminology across the methodology and results discussions while maintaining the original meaning and analytical rigor.

7. DECLARATIONS

7.1. About Authors

Terra Saptina Maulani (TS) https://orcid.org/0009-0008-1106-5674

Dwi Cahyono (DC) https://orcid.org/0000-0001-9951-560X

Yansa Sendi Fadillah (YS) https://orcid.org/0009-0006-8224-5424

Maulidya Reva Aprianti (MR) https://orcid.org/0009-0006-0594-5718

John Edwards (JE) https://orcid.org/0009-0004-0067-0490

7.2. Author Contributions

Conceptualization: TS, and DC; Methodology: YS; Software: TS; Validation: MR and DC; Formal Analysis: YS and TS; Investigation: DC Resources: YS; Data Curation: JE; Writing Original Draft Preparation: DC; Writing Review and Editing: JE; Visualization: MR; All authors, TS, DC, YS, MR and JE, 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] 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] M. S. Rahman, M. Chamikara, I. Khalil, and A. Bouras, "Blockchain-of-blockchains: An interoperable blockchain platform for ensuring iot data integrity in smart city," *Journal of industrial information integration*, vol. 30, p. 100408, 2022.

[3] O. M. Ijiga, S. A. Balogun, N. Okika, O. J. Agbo, and L. A. Enyejo, "An in-depth review of blockchain-integrated logging mechanisms for ensuring integrity and auditability in relational database transactions," *International Journal of Social Science and Humanities Research*, vol. 13, no. 3, pp. 245–259, 2025.

[4] S. Muvva, "Blockchain technology in data engineering: Enhancing data integrity and traceability in modern data pipelines," *IJLRP-International Journal of Leading Research Publication*, vol. 4, no. 7, 2023.

[5] S. Somanathan, "Blockchain for data integrity in multi-cloud environments: a project management approach," *Nanotechnol. Percept*, vol. 20, p. 13, 2024.

[6] Rilis Humas Jabar. (2024, May) West java provincial government implements blockchain technology in the government sector. Accessed: 2026-02-07. [Online]. Available: https://www.jabarprov.go.id/en/berita/pemdaprov-jabar-terapkan-teknologi-blockchain-di-sektor-pemerintahan-13599

[7] K. Diantoro, D. Supriyanti, Y. P. A. Sanjaya, S. Watini *et al.*, "Implications of distributed energy development in blockchain-based institutional environment," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 209–220, 2023.

[8] M. I. Hossain, T. Steigner, M. I. Hussain, and A. Akther, "Enhancing data integrity and traceability in industry cyber physical systems (icps) through blockchain technology: A comprehensive approach," *arXiv preprint arXiv:2405.04837*, 2024.

[9] M. Johns, T. Meurers, F. N. Wirth, A. C. Haber, A. Mueller, M. Halilovic, F. Balzer, and F. Prasser, "Data provenance in biomedical research: scoping review," *Journal of medical Internet research*, vol. 25, p. e42289, 2023.

[10] S. Kosasi, U. Rahardja, N. Lutfiani, E. P. Harahap, and S. N. Sari, "Blockchain technology-emerging research themes opportunities in higher education," in *2022 international conference on science and technology (ICOSTECH)*. IEEE, 2022, pp. 1–8.

[11] M. J. Sembay, D. D. J. de Macedo, L. P. Júnior, R. M. M. Braga, and A. Sarasa-Cabezuelo, "Provenance data management in health information systems: a systematic literature review," *Journal of Personalized Medicine*, vol. 13, no. 6, p. 991, 2023.

[12] M. J. Sembay, D. D. J. de Macedo, and A. A. G. M. Filho, "Identification of the relationships between data provenance and blockchain as a contributing factor for health information systems," in *International Conference on Data and Information in Online*. Springer, 2022, pp. 258–272.

[13] I. P. Gustiah and H. Newell, "Enhancing human resource management efficiency through scalable blockchain networks with an adaptive ai approach," *Startupreneur Business Digital (SABDA Journal)*, vol. 4, no. 2, pp. 114–123, 2025.

[14] C. S. R. Adapa, "Blockchain-based reference data management in healthcare: A technical analysis," *Journal Of Engineering And Computer Sciences*, vol. 4, no. 7, pp. 1260–1267, 2025.

[15] I. Handayani, D. Apriani, M. Mulyati, A. R. A. Zahra, and N. A. Yusuf, "Enhancing security and privacy of patient data in healthcare: A smartpls analysis of blockchain technology implementation," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 1, pp. 8–17, 2023.

[16] J. A. B. Moya, "Blockchain for academic integrity: Developing the blockchain academic credential interoperability protocol (bacip)," *arXiv preprint arXiv:2406.15482*, 2024.

[17] Y. Celik, I. Petri, and M. Barati, "Blockchain supported bim data provenance for construction projects," *Computers in Industry*, vol. 144, p. 103768, 2023.

[18] J. Carlos Ferreira, L. B. Elvas, R. Correia, and M. Mascarenhas, "Enhancing ehr interoperability and security through distributed ledger technology: A review," in *Healthcare*, vol. 12, no. 19. MDPI, 2024, p. 1967.

[19] S. Hussain, H. Rahman, G. M. Abdulsaheb, H. Al-Khawaja, and O. I. Khalaf, "A blockchain-based approach for healthcare data interoperability." *International Journal of Advances in Soft Computing & Its Applications*, vol. 15, no. 2, 2023.

[20] M. Rakhmansyah, M. S. Hadi, S. R. P. Junaedi, F. A. Ramahdan, and S. N. W. Putra, "Integrating blockchain and ai in business operations to enhance transparency and efficiency within decentralized ecosystems," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 157–167, 2025.

[21] E. R. D. Villarreal, J. García-Alonso, E. Moguel, and J. A. H. Alegría, "Blockchain for healthcare management systems: A survey on interoperability and security," *IEEE access*, vol. 11, pp. 5629–5652, 2023.

[22] P. Thantharate and A. Thantharate, "Zerotrustblock: Enhancing security, privacy, and interoperability of sensitive data through zerotrust permissioned blockchain," *Big Data and Cognitive Computing*, vol. 7, no. 4, p. 165, 2023.

[23] E. Uzoma, J. O. Enyejo, and T. M. Olola, "A comprehensive review of multi-cloud distributed ledger integration for enhancing data integrity and transactional security," *International Journal of Innovative Science and Research Technology*, vol. 10, no. 3, 2025.

[24] M. A. Al-Khasawneh, M. Faheem, A. A. Alarood, S. Habibullah, and A. Alzahrani, "A secure blockchain framework for healthcare records management systems," *Healthcare Technology Letters*, vol. 11, no. 6, pp. 461–470, 2024.

[25] M. Lezzi, V. Del Vecchio, and M. Lazoi, "Using blockchain technology for sustainability and secure data management in the energy industry: Implications and future research directions," *Sustainability*, vol. 16, no. 18, p. 7949, 2024.

[26] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 3, no. 2, pp. 168–173, 2023.

[27] P. Tavakoli, I. Yitmen, H. Sadri, and A. Taheri, "Blockchain-based digital twin data provenance for predictive asset management in building facilities," *Smart and Sustainable Built Environment*, vol. 13, no. 1, pp. 4–21, 2024.

[28] I. Khong, N. A. Yusuf, A. Nuriman, and A. B. Yadila, "Exploring the impact of data quality on decision-making processes in information intensive organizations," *APTISI Transactions on Management*, vol. 7, no. 3, pp. 253–260, 2023.

[29] 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.

[30] D. Indiyati, U. Rahardja, U. Rusilowati, S. Millah, A. Faturahman, and A. Fitriani, "Enhancing human resources management with blockchain technology: A case study approach," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.

[31] O. Zorlu and A. Ozsoy, "A blockchain-based secure framework for data management," *IET Communications*, vol. 18, no. 10, pp. 628–653, 2024.

[32] A. Sutarman, E. Kallas, and O. Jayanagara, "The effectiveness of using blockchain technology as a machine learning program," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 29–34, 2024.

[33] S. Terzi and I. Stamelos, "Architectural solutions for improving transparency, data quality, and security in ehealth systems by designing and adding blockchain modules, while maintaining interoperability: the ehdsi network case," *Health and Technology*, vol. 14, no. 3, pp. 451–462, 2024.

[34] Ö. Karaduman and G. Gülhas, "Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand," *Applied Sciences*, vol. 15, no. 9, p. 5168, 2025.

[35] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. Shao, "A survey of blockchain data management systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 21, no. 3, pp. 1–28, 2022.

[36] A. S. Elnara, B. M. Elvan, D. P. Emine, and F. A. Saraswati, "Applications for systematic smart contracts on blockchain," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 1–6, 2023.

[37] C. S. Götz, P. Karlsson, and I. Yitmen, "Exploring applicability, interoperability and integrability of blockchain-based digital twins for asset life cycle management," *Smart and Sustainable Built Environment*, vol. 11, no. 3, pp. 532–558, 2022.

[38] K.-H. Yeh, G.-Y. Yang, C. Butpheng, L.-F. Lee, and Y.-H. Liu, "A secure interoperability management scheme for cross-blockchain transactions," *Symmetry*, vol. 14, no. 12, p. 2473, 2022.

[39] S. K. Rana, S. K. Rana, K. Nisar, A. A. Ag Ibrahim, A. K. Rana, N. Goyal, and P. Chawla, "Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare," *Sustainability*, vol. 14, no. 15, p. 9471, 2022.

[40] M. Elkhodr, S. Khan, and E. Gide, "A novel semantic iot middleware for secure data management: Blockchain and ai-driven context awareness," *Future Internet*, vol. 16, no. 1, p. 22, 2024.

[41] K. Tiwari and S. Kumar, "A healthcare data management system: blockchain-enabled ipfs providing algorithmic solutions for increased privacy-preserving scalability and interoperability," *The Journal of Supercomputing*, vol. 81, no. 8, p. 895, 2025.

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

[43] D. Hossain, Q. Mamun, and R. Islam, "Unleashing the potential of permissioned blockchain: addressing privacy, security, and interoperability concerns in healthcare data management," *Electronics*, vol. 13, no. 24, p. 5050, 2024.

[44] S. Singh, S. K. Sharma, P. Mehrotra, P. Bhatt, and M. Kaurav, "Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives," *Materials Today: Proceedings*, vol. 62, pp. 5042–5046, 2022.

[45] M. Murod, S. Anhar, D. Andayani, A. Fitriani, and G. Khanna, "Blockchain based intellectual property management enhancing security and transparency in digital entrepreneurship," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 240–251, 2025.

[46] M. Hardini, V. Agarwal, D. Apriani, I. A. Widjaya, E. Setiawaty, and N. Nurasiah, "Application of database normalization in increasing data storage efficiency," *International Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 201–211, 2025.

[47] S. El Haddouti, A. Ouaguid, and M. D. Ech-Cherif El Kettani, "Fedidchain: An innovative blockchain-enabled framework for cross-border interoperability and trust management in identity federation systems," *Journal of Network and Systems Management*, vol. 31, no. 2, p. 42, 2023.

[48] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble, and R. A. Dziyauddin, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023.

[49] S. Staynov, "A blockchain-driven approach for secure and scalable provenance management in open data systems," Ph.D. dissertation, Technische Universität Wien, 2023.

[50] M. H. Mughal, Z. A. Shaikh, K. Ali, S. Ali, and S. Hassan, "Ipfs and blockchain based reliability and availability improvement for integrated rivers' streamflow data," *IEEE Access*, vol. 10, pp. 61 101–61 123, 2022.

[51] D. Wong You King, M. A. Riza, L. Kok Leong, U. H. Mohamad, R. A. Kadir, M. F. Zulkifli, and M. N. Ahmad, "Blockchain-enhanced traceability framework for smart farming with integrated ontology-based data standardization." *International Journal on Advanced Science, Engineering & Information Technology*, vol. 14, no. 4, 2024.