Teknik: Jurnal Ilmu Teknik dan Informatika
Volume 5 Nomor 1 Mei 2025
e-ISSN: 2798-2513; p-ISSN: 2808-8751, Hal 126-133
DOI: https://doi.org/10.51903/teknik.v5i1.891
Available online at: https://journal.stiestekom.ac.id/index.php/TEKNIK

Leveraging Blockchain Technology to Enhance Data Integrity and Transparency in Government Data Centers

Adi Affandi Rotib[1] , Silviana Windasari[2*], Bayu Bagaskoro[3], Ade Frihadi[4], Abdurohman[5]
[1234]Department of Electrical Engineering, Faculty of Engineering, Universitas Sains Indonesia, Indonesia
[5]Graduate School of Electrical Engineering - School of Bioscience, Technology and Innovation (SBTI) Atma Jaya Catholic University of Indonesia, Indonesia
Email: *silviana.windasari@lecturer.sains.ac.id*.

Address: Jl. Akses Tol No.50, Gandasari, Kec. Cibitung, Kabupaten Bekasi, Jawa Barat 11650
Author correspondence: silviana.windasari@lecturer.sains.ac.id.

Abstract*. Government data centers in Indonesia face significant challenges related to data integrity and transparency, impacting policy-making accuracy, operational efficiency, and public trust. Data fragmentation, information inconsistency, and vulnerability to manipulation and cyberattacks have become crucial issues. Blockchain technology, with its fundamental characteristics such as decentralization, immutability, cryptography, and consensus mechanisms, offers innovative solutions to address these problems. This research employs a systematic literature review and conceptual analysis approach to identify how blockchain principles can be effectively applied. The proposed conceptual model, which utilizes permissioned blockchains like Hyperledger Fabric and distributed storage systems such as the InterPlanetary File System (IPFS), demonstrates significant potential in creating a secure, transparent, and auditable data ecosystem. Blockchain implementation is expected to enhance data security, strengthen auditability, prevent fraud, improve operational efficiency, securely manage digital identities, and increase data availability and redundancy. Although implementation challenges exist, including technical complexity, immature regulations, costs, and human resource gaps, global case studies and initial initiatives in Indonesia indicate significant feasibility and benefits. This report recommends a holistic approach encompassing adaptive regulatory development, infrastructure and human resource investment, phased pilot projects, and multi-stakeholder collaboration to realize blockchain's full potential in improving government data governance.*
Keywords*: Blockchain, Cybersecurity, Data Integrity, Data Transparency, Government Data Center*

1. INTRODUCTION

In modern governance, data is a vital asset for formulating effective policies and delivering high-quality public services (Rajasekaran et al., 2022), (Dong et al., 2023), (Zubaydi et al., 2023), (Eghmazi et al., 2024) . In Indonesia, data plays a central role in national development planning across sectors such as economy, social affairs, education, and health. However, data management within government data centers still faces fundamental challenges, including fragmentation among ministries and agencies that leads to duplication, inconsistency, and unsynchronized information. This situation undermines the reliability of data as a foundation for accurate decision-making. Gaps in technology infrastructure, human resource skills, and regulatory frameworks between central and regional governments further exacerbate the problem, resulting in poor data quality, misguided policies, and diminished public trust. Cybersecurity threats, such as the LockBit 3.0 ransomware attack that disrupted hundreds of government institutions, highlight the persistent vulnerability of the nation’s digital infrastructure.

Blockchain technology has emerged as a transformative solution for addressing these issues, offering strong guarantees in data transparency, immutability, and decentralized control. In public administration, where sensitive data flows across multiple departments and jurisdictions, blockchain allows for secure and verifiable transactions (Duvvur, 2024). Government IT infrastructures are now leveraging blockchain to mitigate data fraud, enhance

Received: July 9, 2025; Revised: August 9, 2025; Accepted: August 18, 2025; Online Available: August 23, 2025; Published: August 25, 2025

regulatory compliance, and automate audit trails through smart contracts and consensus mechanisms (Patel et al., 2024), (Pratama et al., 2024). The Indonesian government's increasing focus on smart governance and digital resilience has fueled interest in blockchain-based data centers for reliable public service delivery (Gunawan & Sharma, 2025)(Ungson & Soorapanth, 2022). Its decentralized architecture eliminates single points of failure, minimizes manipulation risks, and ensures that once data is stored, it remains tamper-proof.

The relevance of blockchain expands further into validating real-time digital environments, such as digital twins used for public infrastructure simulations. Blockchain validation ensures synchronization between physical and virtual assets(Ferone & Verrilli, 2025), while secure recordkeeping ensures historical consistency and trust(Le et al., 2023), (Setiawan & Sutabri, 2025). Case implementations in Indonesia like Pemkot Bekasi's blockchain integration and BPS's use of blockchain for population data illustrate real-world confidence in this technology (Amazon, n.d.), (Sukmawijaya & Gunanto, 2023). Furthermore, blockchain-based models in public health insurance have enhanced privacy, traceability, and citizen data ownership (Setiawan & Sutabri, 2025), while cyber-resilient architectures based on blockchain reinforce protection against manipulation and hacking attempts (Pixelfield, 2025).

To ensure successful implementation, this study outlines not only technical aspects of blockchain, but also strategic dimensions such as regulatory frameworks, inter-agency collaboration, and skill development. Blockchain auditing systems have strengthened transparency in budgeting and public finance management (Septania Parapat et al., 2025), (Pratama et al., 2024), while conceptual models from UDBS and blockchain-based record control (Setiawan & Sutabri, 2025) present practical pathways for adoption. Still, challenges remain regarding interoperability with legacy systems and nationwide scalability. Therefore, this study proposes a blockchain-based architecture tailored for government data centers, supported by case analysis and recommendations, to optimize data governance, ensure data accuracy, and restore public trust in digital public services.

2. THEORETICAL FRAMEWORK

This research is grounded in data governance theory, trust and transparency in e-government, and New Public Management (NPM), emphasizing the strategic management of data as a valuable asset through transparency, accountability, and the integration of technology to enhance public service efficiency. Effective data governance entails regulatory compliance, data quality improvement, protection of sensitive information, and interagency collaboration, despite persistent challenges such as fragmented systems, inconsistent standards, and limited resources. Theories on trust and transparency highlight that digital technology adoption can strengthen openness, public participation, and positive societal perceptions, while NPM promotes the adoption of private-sector principles to improve public sector performance. Blockchain, with its decentralization, immutability, cryptography, and consensus mechanisms, is regarded as a means to address cybersecurity vulnerabilities, reduce manipulation risks, and build public trust through transparency and traceability. Global case studies such as Estonia’s KSI blockchain for health and e-Residency records, Georgia’s blockchain-based land registry, and Sweden’s digital property certificatesdemo nstrate its potential in the public sector. In Indonesia, although adoption is still in its early stages, initiatives such as the Central Bureau of Statistics’ use of blockchain for population data processing and Bekasi Regency’s deployment to prevent data leaks indicate promising development. Drawing upon these theoretical foundations and empirical evidence, this research proposes a hybrid architecture combining permissioned blockchain with distributed storage to enhance data integrity and transparency in government data centers, thereby strengthening public trust and operational efficiency.

3. RESEARCH METHODOLOGY

This study adopts a Systematic Literature Review (SLR) approach to gather, evaluate, and synthesize information from diverse academic and industry sources on the use of blockchain technology to improve data integrity and transparency in government data centers. Data were collected from Scopus- and SINTA-indexed journals, research reports from reputable institutions, news articles from credible media, and official publications from government agencies and international organizations focusing on blockchain, data governance, and the public sector. A systematic search was conducted using keywords such as "blockchain," "data integrity," "data transparency," "government data center," "e-governance," "Indonesia," "data governance," "cybersecurity," "blockchain architecture," "smart contracts," and "case studies." The qualitative analysis identified key themes, patterns, benefits, challenges, and proposed conceptual models, synthesizing fragmented insights into a coherent framework that examines both strategic and practical implications of blockchain adoption. The assessment of blockchain's potential employed an analytical framework incorporating data evaluation criteria and parameters for determining the feasibility of implementing this technology in the public sector.

Analytical Framework

This study employs a comprehensive analytical framework to evaluate the potential of blockchain in enhancing data integrity and transparency within government data centers, encompassing criteria such as accuracy, consistency, completeness, timeliness, auditability, public verifiability, and resistance to manipulation. Feasibility parameters for blockchain adoption in the public sector include security, transparency, efficiency, scalability, interoperability, data privacy, regulatory and governance support, and the readiness of human resources and organizational culture. A paradigm shift from "perimeter" security to "data-centric" protection is essential, wherein blockchain's cryptographic security and immutability safeguard data against tampering even if the host system is compromised. Nevertheless, successful implementation depends not solely on technical capacity but also on a holistic evaluation of legal, economic, social, and cultural dimensions. Neglecting any of these aspects risks undermining the initiative regardless of the technology's strengths, making this framework the foundation for the in-depth analysis presented in the discussion section.

4. RESULT AND DISCUSSION

The implementation of blockchain technology to enhance data integrity and transparency in government data centers is grounded in core principles that set it apart from traditional database systems decentralization, immutability, cryptography, and consensus mechanisms which collectively establish a secure, trustworthy, and accountable data ecosystem. Decentralization eliminates single points of failure by distributing control and encrypted data across multiple network nodes, thereby reducing vulnerability to unauthorized access or manipulation. Immutability ensures that once data is recorded, it cannot be altered or deleted, preserving a permanent and verifiable audit trail. Cryptographic techniques safeguard the confidentiality, authenticity, and integrity of data, while consensus mechanisms enable all participants in the network to agree on a single, consistent version of the truth, even in environments where trust among parties is limited. The synergy of these principles not only addresses challenges such as data fragmentation, manipulation, and interagency distrust but also shifts the paradigm from reliance on institutional authority to confidence in system design, thereby fostering higher levels of public trust in government data governances.

The application of blockchain technology to enhance data integrity and transparency in government data centers is founded on four core principles decentralization, immutability, cryptography, and consensus mechanisms which differentiate it from traditional database systems. Decentralization eliminates single points of failure by encrypting and distributing data across network nodes, making unauthorized manipulation or access far more difficult.

Immutability ensures that once data are recorded, they cannot be altered or deleted, with each block cryptographically linked to maintain a transparent audit trail. Cryptography safeguards data using hashing, public-key encryption, and digital signatures to verify authenticity and security. Consensus mechanisms ensure that all nodes share an identical transaction history and prevent misuse. The integration of these principles creates a secure, transparent, and trustworthy data ecosystem critical for addressing government challenges such as data silos, manipulation, and interagency distrust.

The conceptual model for blockchain integration in government data centers combines permissioned blockchain platforms such as Hyperledger Fabric with distributed storage systems like IPFS, enabling strict access control for sensitive data and efficient storage for large datasets. A web-based portal serves as the user interface for data uploads, metadata verification, and IPFS storage, while the blockchain immutably records hashes and activity logs. Smart contracts are employed to automate processes, enforce rules, and enhance transparency in public services, including digital identity management, budget allocation, and procurement. This hybrid approach not only strengthens security and auditability but also reduces operational costs and reliance on centralized infrastructure. Thus, blockchain serves not merely as a supporting technology but as a foundation for institutional reform, accelerating the digital transformation of governance.The following Table 1 provides a concise comparison between the challenges of traditional data governance and how blockchain offers corresponding solutions.

Table 1. Comparison of Traditional Data Governance Challenges vs. Blockchain Solutions

Challenge Category	Traditional Systems	Blockchain Solutions
Data Fragmentation	Data silos between government agencies, with separate management practices	Distributed ledger ensuring consistent copies across all nodes
Data Inconsistency	Duplication and inconsistency of information	Consensus mechanisms ensuring a unified view of data
Data Manipulation	Data alterations without clear traceability, coupled with weak oversight mechanisms	Immutability and cryptographic audit trails enabling
Lack of Transparency	Outdated or incomplete reports, leading to public distrust	Transparent ledger with public verification and audit trails
Single Point of Failure	Reliance on a central authority/server, vulnerable to targeted attacks	Decentralization, with data distributed across multiple nodes
Low Public Trust	Non-transparency fostering suspicions of corruption and questionable policy decisions	Trust by design, enabling proactive accountability

Manual Audit Processes	Time-consuming, costly, and prone to human error	Automated auditability with permanent audit trails
Corruption Potential	Opportunities for budget misuse due to inadequate oversight	Smart contracts enabling transparent budget tracking

Case Studies on Blockchain Implementation in the Public Sector

The adoption of blockchain technology in the public sector has demonstrated its transformative potential in various countries, including early-stage initiatives in Indonesia. This section presents case studies that provide tangible illustrations of how blockchain can enhance the integrity and transparency of government data.

Global Case Studies

Estonia: Recognized as a pioneer in digital governance, Estonia has implemented blockchain technology on a national scale. The e-Estonia initiative employs KSI blockchain to ensure that networks, systems, and data remain uncompromised, while maintaining full data privacy. Blockchain is utilized to secure over one million citizens' health records, validate transactions through a decentralized ledger, and manage the e-Residency program, which enables secure access to public services.

Georgia: To address long-standing property dispute issues, the Government of Georgia implemented a blockchain-based land registry. By 2018, over 1.5 million land titles had been registered on the blockchain, enabling citizens to obtain digital certificates with timestamps and cryptographic proof of ownership. This system has significantly improved transparency, security, and reduced corruption in land administration.

Sweden: In early 2017, the Swedish Mapping, Cadastre, and Land Registration Authority initiated a conceptual project to record land title information and real estate transactions using blockchain. The objectives included accelerating transactions, enhancing transparency, eliminating multiple property sales, and strengthening security through independent verification.

United States:

a. The Department of Homeland Security (DHS) has led experimental initiatives utilizing blockchain and Distributed Ledger Technology (DLT) to improve operational transparency, auditability of public services, supply chain visibility, and automation of paper-based processes. The focus includes issuing and verifying digital credentials, managing certificates, and enabling decentralized identities.
b. west Virginia successfully piloted blockchain-based voting for absentee voters to enhance transparency and reliability in public elections.
c. The City of Baltimore introduced blockchain technology to monitor over 15,000 vacant homes, record more than 200,000 land titles and property assessments, track permits, and streamline processes for purchasing vacant properties.

Brazil: Implemented blockchain to increase transparency in tax reporting, serving as a model for other nations.

Dubai: Aspiring to become the world's first blockchain-powered government, Dubai's Smart Dubai initiative aims to digitize all applicable documents and transactions. The program uses blockchain for land registration, reducing fraud, paperwork, and inefficiencies in property transactions.

Case Studies in Indonesia

Although blockchain adoption in Indonesia's public sector remains in its early stages, several initiatives and plans demonstrate growing awareness of its potential:

One Data Indonesia (Satu Data Indonesia – SDI): While SDI is not itself a blockchain implementation, its primary objective to integrate cross-sectoral data and improve data quality

aligns closely with blockchain's capabilities to produce accurate, up-to-date, unified, and accountable data. Blockchain could serve as a powerful enabling technology to achieve SDI's principles.

Central Statistics Agency (Badan Pusat Statistik – BPS): BPS Head Margo Yuwono has announced plans to leverage blockchain technology for processing Indonesia's population data (Social and Economic Registration/Regsosek). The goal is to enhance data accuracy, accountability, and traceability, in line with Presidential Regulation No. 132 of 2022 on the National Electronic-Based Government System (SPBE) Architecture. This represents a significant step toward applying blockchain in national statistical data management.

Bekasi Regency Government: Plans are underway to deploy blockchain to prevent government data breaches, particularly in systems such as online school admissions (PPDB Online), civil service, population records, yellow card issuance, and the Bebunge application. This reflects local-level recognition of blockchain's role in safeguarding data security.

Ministry of Health: The Chief Digital Transformation Office of the Ministry of Health has participated as a panelist in discussions on cross-sector blockchain implementation, signaling exploration of blockchain's potential in health data management.

Other Potential Applications: Literature also highlights explorations of blockchain use in Indonesia for archival systems to enhance data security and integrity, value-added tax (VAT) reporting, distribution of COVID-19 social assistance funds, and optimization of smart contracts for digital certification systems.

Lessons from these implementations indicate that successful blockchain adoption often begins with high-impact, specific use cases such as land registries or identity management rather than a full-scale system overhaul. These experiences also emphasize the importance of government leadership, collaboration with the private sector, and a clear regulatory environment. This suggests that a phased, collaborative approach is likely to be the most feasible path for Indonesia.

Challenges in Implementing Blockchain within Indonesia's Government Data Centers

While blockchain technology offers substantial potential to enhance data integrity and transparency in Indonesia's government data centers, its implementation faces multifaceted challenges requiring strategic resolution. On the technical side, integrating blockchain with traditional database systems demands significant architectural redesign and adjustments due to differences in data structures and operational mechanisms. Scalability remains a key issue, particularly for large-scale, real-time data processing, thus necessitating hybrid architectures such as off-chain storage solutions using IPFS. Additional challenges include interoperability across blockchain platforms, the absence of standardized communication protocols, and disparities in technological infrastructure across regions. From a regulatory perspective, Indonesia's blockchain legal framework remains largely limited to cryptocurrency assets, lacking comprehensive provisions for data security, consumer protection, and technical standards in the public sector. High implementation costs for hardware, software, application development, and workforce training pose further obstacles, especially given the shortage of blockchain-skilled professionals and uneven digital literacy between central and regional governments.

Non-technical challenges involve organizational culture shifts and public acceptance, both of which require strong leadership to promote transparency. Resistance may stem from reluctance to share information or a lack of understanding of its benefits, while public trust hinges on consistent transparency and education about blockchain's advantages and security. Striking a balance between transparency and personal data privacy is also critical, particularly in safeguarding citizens' sensitive information. Potential solutions include implementing permissioned blockchains with strict access controls, coupled with advanced encryption and data anonymization techniques. Addressing these challenges calls for balanced policy

frameworks stringent enough to protect data security and privacy, yet flexible enough to foster innovation and ecosystem growth. Overly restrictive regulations risk stifling adoption, while overly lenient policies could expose systems to vulnerabilities and misuse.

Addressing these challenges calls for an open innovation framework and multi-stakeholder collaboration. Close cooperation between government, industry, and academia is essential to identify and develop pilot projects that can clearly demonstrate blockchain's benefits. Such collaboration will create an enabling ecosystem for smart contract development and blockchain adoption, ensuring that implemented solutions are practical, sustainable, and widely accepted.

5. CONCLUSION AND RECOMMENDATION

Indonesia's government data centers continue to face major challenges in maintaining data integrity and transparency, including fragmentation, inconsistent information, potential manipulation, and cybersecurity threats that undermine policy quality, operational efficiency, and public trust. Blockchain technology offers a promising solution through its core attributes decentralization, immutability, cryptography, and consensus mechanisms. Decentralization removes single points of failure, while immutability ensures that once data is recorded, it cannot be altered, leaving a permanent audit trail. Cryptography protects data confidentiality and authenticity, while consensus mechanisms enable reliable agreement among network nodes. This synergy shifts the paradigm from "trust in authority" to "trust in design," which is essential for restoring public confidence. The proposed conceptual model combines a permissioned blockchain such as Hyperledger Fabric with distributed storage using IPFS, where blockchain safeguards the integrity of metadata and transaction logs, while IPFS stores actual data in a distributed manner to address scalability and cost constraints. Integration with existing systems can be achieved via APIs, and smart contracts can automate government processes, improving efficiency and reducing opportunities for corruption.

The adoption of blockchain in government data centers could yield significant benefits, including enhanced data security, greater transparency and auditability, fraud prevention, improved operational efficiency, and cost savings by reducing intermediaries and expediting processes. It also enables secure digital identity management and ensures data availability through replication across multiple nodes. However, challenges such as technical complexity, scalability limitations, lack of comprehensive regulations, high initial costs, human resource skill gaps, and resistance from organizational culture and the public must be addressed. Strategic measures include establishing a clear and adaptive regulatory framework prioritizing security, privacy, and technical standards; investing in IT infrastructure and human resource development; starting with small-scale, high-impact pilot projects; fostering cross-sector collaboration; designing systems with strong privacy safeguards; and promoting public education to build awareness and trust. By following these steps, Indonesia can progressively develop government data centers that are more secure, transparent, efficient, and trustworthy strengthening the foundation for a smart and accountable digital government.

REFFERENCES

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. *PeerJ Computer Science*, *9*, e1705.

Duvvur, V. (2024). Modernizing Government IT Systems: A Case Study on Enhancing Operational Efficiency and Data Integrity. *International Journal of Computational and Experimental Science and Engineering*, *11*(1), 10–22399.

Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. *IoT*, *5*(1), 20–34. https://doi.org/10.3390/iot5010002

Ferone, A., & Verrilli, S. (2025). Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency. *Future Internet*, *17*(1), 31.

Gunawan, W., & Sharma, D. (2025). Mapping Public Interest in Cryptocurrency in Indonesia (2021--2024): Analyzing Geographical Disparities and Temporal Trends. *Blockchain, Artificial Intelligence, and Future Research*, *1*(1), 13–22.

Le, N. T., Thwe Chit, M. M., Truong, T. Le, Siritantikorn, A., Kongruttanachok, N., Asdornwised, W., Chaitusaney, S., & Benjapolakul, W. (2023). Deployment of Smart Specimen Transport System Using RFID and NB-IoT Technologies for Hospital Laboratory. *Sensors*, *23*(1), 1–13. https://doi.org/10.3390/s23010546

Patel, K., Chauhan, D., Mishra, P., Rath, J. J., Saxena, K. K., Prasad, K. S. R., & Bandhu, D. (2024). Design and development of a modular hydroponic tower with topology optimization. *International Journal on Interactive Design and Manufacturing*, *333*(24), 1–10. https://doi.org/10.1007/s12008-024-02052-1

Pixelfield. (2025). *Cryptography in Blockchain: What Is It And How Does It Work?* https://pixelfield.co.uk/blog/cryptography-in-blockchain/

Pratama, R. Y., Janah, T. N., Rahardiansyah, R. A., & Pramono, P. (2024). Pengembangan Model Konseptual Integrasi Blockchain untuk Meningkatkan Keamanan dan Integritas Data dalam Sistem Kearsipan. *Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis*, 545–549.

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039.

Septania Parapat, E. P., Siringi ringo, E. D., & Siahaan, J. (2025). Kerangka Audit Real-Time Berbasis Blockchain untuk Tata Kelola Keuangan Sektor Publik di Indonesia: Studi Kasus Tantangan Implementasi IPSAS dan Reformasi Kelembagaan. *JUMMA'45: Jurnal Mahasiswa Manajemen Dan Akuntansi*, *4*(1), 318–331.

Setiawan, R., & Sutabri, T. (2025). Integrasi Teknologi Blockchain untuk Kontrol Akses yang Aman dalam Basis Data Terdistribusi. *JOURNAL SAINS STUDENT RESEARCH*, *3*(2), 379–384.

Sukmawijaya, A., & Gunanto, A. A. (2023). *BPS Bakal Gunakan Blockchain untuk Olah Data Penduduk*. https://kumparan.com/kumparanbisnis/bps-bakal-gunakan-blockchain-untuk-olah-data-penduduk-1zjrMjf42pG/full

Ungson, G. R., & Soorapanth, S. (2022). The ASEAN blockchain roadmap. *Asia and the Global Economy*, *2*(3), 100047.

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. *Sensors*, *23*(2), 788.