JURNAL BINA PRAJA
Journal of Home Affairs Governance

ARTICLE

Blockchain Adoption Readiness

Expert Perspectives on Policy, Implementation, and Governance in Indonesia

Juan Mikael Simatupang [1], **Etin Indrayani** [2]

[1, 2]Faculty of Government Management, Institut Pemerintahan Dalam Negeri

juanspansa33@gmail.com

OPEN ACCESS

Citation: Simatupang, J. M., & Indrayani, E. (2025). Blockchain Adoption Readiness: Expert Perspectives on Policy, Implementation, and Governance in Indonesia. *Jurnal Bina Praja, 17*(3). https://doi.org/10.21787/jbp.17.2025-2681

Submitted: 14 August 2025

Accepted: 23 October 2025

Published: 31 December 2025

Abstract: Indonesia faces serious cybersecurity challenges due to its centralized data systems, which are vulnerable to attack. Blockchain technology offers potential solutions through its decentralized, immutable, and transparent architecture. This study examines the readiness for blockchain adoption in Indonesia using a qualitative approach through in-depth interviews with purposively selected experts from government, academia, and non-governmental organizations. The results indicate that the fundamental challenges are non-technical. Legally, blockchain's immutable nature conflicts with citizens' right to delete personal data, while policy-wise, the principle of decentralization is inconsistent with the government's mandate for data centralization. The findings suggest that the primary obstacles are not technical issues, but rather a lack of political will, bureaucratic resistance, and budget constraints. Therefore, the most realistic solution for Indonesia is the implementation of a permissioned blockchain model. This model must be designed with privacy-by-design principles and must comply with national cybersecurity standards to be implemented amidst existing legal and policy challenges.

Keywords: Blockchain; Cybersecurity; Government; Permissioned Blockchain; Public Policy.

1. Introduction

Indonesia's digital transformation is experiencing significant progress. This accelerated digitalization, aimed at increasing efficiency and transparency, has indirectly expanded the attack surface for crucial government data infrastructure. A report from the National Cyber and Crypto Agency (BSSN) indicates an increasing trend in cyberattacks targeting government systems, reaching 290 million attacks in 2020 and continuing to grow in subsequent years, with the administrative sector being a primary target (Chotimah, 2016). Major security incidents, such as the BPJS Kesehatan data leak and the ransomware attack on Bank Syariah Indonesia, highlight vulnerabilities that threaten national data sovereignty. Therefore, the need for improved cybersecurity governance is urgent to address these challenges (Primawanti & Pangestu, 2020).

The root of these vulnerabilities lies in the reliance on traditional, centralized data management architectures. These systems are inherently fragile, vulnerable to single points of failure, and not designed to withstand modern, distributed, and persistent cyber threats. The failure of a single central server can cripple widespread services and open up access for malicious actors to exploit data on a massive scale. Therefore, a shift towards a more decentralized and autonomous model is increasingly important. Implementing a model that leverages blockchain technology can provide a more robust solution to cybersecurity challenges by providing redundancy and greater resilience to cyberattacks (Makhdoom et al., 2019). However, it is important to note that there are challenges and issues that need to be addressed along with blockchain adoption, especially in the context of the Internet of Things (IoT) and broader decentralized architectures (Makhdoom et al., 2019). Thus, implementing this innovation is a crucial step to strengthen digital infrastructure and maintain the integrity of public data in Indonesia.

It is in this context that blockchain technology offers an alternative paradigm. Blockchain is a distributed ledger technology that records transactions in cryptographically linked blocks of data (Zheng et al., 2017). Its main characteristics include decentralization (not dependent on a central authority), immutability (recorded data is difficult to change), and transparency (can be verified by authorized parties) (Zhang et al., 2021). There are several types of blockchain, including public blockchain (open to all) and permissioned blockchain (only authorized parties can access), which have different socio-technical and political implications (X. Xu et al., 2017). With its core principles of decentralization, cryptographic immutability, and transparency, blockchain offers an architecture that is fundamentally more resilient to centralized manipulation and attacks. These characteristics directly address the inherent weaknesses of current government data systems, positioning it as a promising technological solution. Research shows that blockchain implementation in the public sector can reduce the cost and complexity of information exchange, increase transparency and accountability, and reduce corruption and abuse of power (Akhmetbek & Špaček, 2021; Allessie et al., 2019). Furthermore, the implementation of blockchain architecture allows for a verifiable transaction trail, significantly increasing trust between the government and citizens. Given this potential, blockchain is considered an innovation that could transform the way governments manage and protect public data.

Table 1. Summary of Cyber Security Incidents in Indonesia

Incident	Year	Affected Entities	Description and Impact	Systemic Vulnerabilities Exposed
BPJS Health Data Leak	2021	279 million Indonesian population	Selling highly sensitive personal data (Population Identification Number, salary, etc.) online	Data encryption failures at rest, weak access controls, and lack of security audits on massive databases.

Incident	Year	Affected Entities	Description and Impact	Systemic Vulnerabilities Exposed
Hacker Action of "Bjorka"	2022	Various state institutions (General Election Commission, Ministry of Communication and Digital, State Intelligence Agency)	Leaking of driver's license registration data, voter data, and confidential state documents. Doxing of public officials.	Data security fragmentation between agencies, inadequate protection of sensitive data, and slow incident response.
BSI Ransomware Attack	2023	Bank Syariah Indonesia (BSI)	Days of banking outage, the theft of 1.5 TB of customer data, and a $20 million ransom demand.	Weaknesses in network segmentation, poor patch management, and lack of a reliable disaster recovery plan.
PDN Ransomware Attack	2024	Hundreds of central and regional government agencies	The total paralysis of the National Data Center, disrupting more than 200 crucial public services.	Extreme risks from centralization without layered protection, weak security configurations, and reliance on a single point of failure.

Source: *Data processed from BSSN reports (2021-2024) and national news*

Therefore, this study aims to comprehensively analyze the potential and challenges of implementing blockchain technology as an instrument for transforming government data security in Indonesia. This study is based on a significant research gap, where in-depth analysis of the feasibility of blockchain implementation that takes into account the unique socio-technical context, legal framework, and bureaucratic culture in Indonesia is still very limited. This study is crucial because adopting technology without a deep contextual understanding risks clashing with national regulatory pillars and can hinder successful implementation. Therefore, this analysis is expected to bridge this knowledge gap and provide guidance for more effective implementation strategies in Indonesia (Hayes, 2019; Wijaksono et al., 2022). The analytical approach in this study integrates secondary and primary data in a step-by-step manner. The foundation of the analysis is built by mapping the cyberthreat landscape and systemic vulnerabilities using secondary data such as official reports and case studies, complemented by a technical deconstruction of blockchain solutions based on a literature review. On top of this foundation, primary data from in-depth interviews with experts is used to qualitatively analyze various non-technical challenges—including policy, bureaucratic, and political will—impacting the implementation of this technology in the Indonesian government context (Daliya & Bhandari, 2024). Next, this article will evaluate global implementation case studies to draw relevant lessons and conclude with a strategic framework and contextual policy recommendations for Indonesia, including how blockchain can be applied in public data archiving and management (Wijaksono et al., 2022).

2. Methods

This study uses a qualitative approach to provide an in-depth understanding of the implementation of blockchain technology in government data security (Lykidis et al., 2021). The design used a descriptive-analytical case study to describe the phenomenon, analyze the relationship between variables, and identify challenges and opportunities (Difrancesco et al., 2023).

Data collection was conducted through primary and secondary sources. Primary data were obtained from in-depth interviews and Focus Group Discussions (FGDs) with five key informants. Informants were selected using purposive sampling based on their relevance and expertise (Zahra & Amaliyah, 2023). The informant profiles included representatives from the National Cyber and Crypto Agency (BSSN) Cryptographer Division, the Director of Public Communications at the Ministry of Communication and Digital, academics focusing on technology policy, and representatives from non-governmental organizations working in the field of government transparency. Snowball sampling techniques were also used to reach other relevant informants. The interview protocol used a semi-structured guide that focused on three main aspects:

(1) policy and regulatory analysis, (2) institutional and governance readiness, and (3) identification of implementation challenges and opportunities (Marlina et al., 2023).

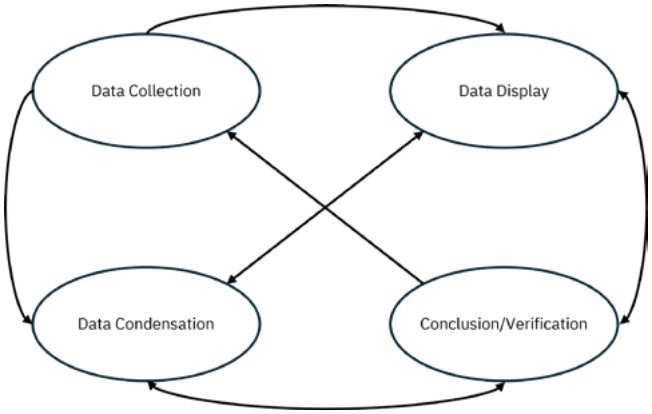

Figure 1. Miles and Huberman's Interactive Model

Data analysis applies Miles and Huberman's interactive model, which consists of three stages. First, data reduction, which involves filtering the collected raw data to focus on relevant information (Adawiah et al., 2023; Sinaga & Putra, 2021). Second, data presentation, where the reduced data is presented systematically in the form of narrative text and tables to facilitate analysis (Adawiah et al., 2023; Sinaga & Putra, 2021). Third, drawing conclusions, namely compiling research findings based on data that has been analyzed to answer the problem formulation (Firman, 2018).

3. Results and Discussion

Blockchain technology, with its fundamentally decentralized, immutable, and transparent nature, offers transformative potential to revolutionize data security and governance in the public sector. This concept promises to create a more accountable, efficient, and secure government free from manipulation (Muhamediyeva & Khudoyberdiev, 2023). However, the successful adoption of this disruptive technology depends heavily on a country or organization's level of Blockchain Adoption Readiness. This readiness is a multidimensional concept that goes beyond the mere availability of technological infrastructure to encompass policy readiness, human resources, budgets, and socio-political factors that influence an entity's ability to effectively utilize this technology (Chen & Lloyd, 2021; Ejairu et al., 2024). Factors such as competitive pressure, complexity, and cost have also been identified as significant influences in blockchain adoption, particularly in the public sector, which has its own challenges in implementing this new technology (Ejairu et al., 2024; Gong et al., 2022).

Studies on technology adoption readiness, such as those conducted in this study, are highly relevant to the findings of various sources. As highlighted by experts in interviews, the implementation of advanced technologies in developing countries tends to focus not only on the technical environment but also requires in-depth consideration of organizational aspects, policies, and political will (Saif et al., 2022). The findings of this study confirm that leadership commitment and a clear regulatory framework have a significant impact on the success of blockchain implementation, while resistance to change, cultural challenges, and budget politics are the main barriers (Saif et al., 2022; Tak, 2023). The analysis of the results of this study will critically examine the various dimensions of this readiness, with a focus on the factual conditions in the Indonesian government based on the collected data (Falcone et al., 2021; Saif et al., 2022).

3.1. Blockchain Implementation Policy

Indonesia's regulatory landscape provides a legal foundation that indirectly enables the adoption of blockchain technology in the public sector. Its main pillar is Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, which provide legal recognition and force for electronic documents and electronic signatures (Baihaiqi et al., 2022; Muko, 2024). This foundation is essential because it legitimizes immutable transaction records and smart contracts in the blockchain as legally accountable evidence (Suwardiyati et al., 2024). This foundation is strengthened by the cybersecurity framework of the National Cyber and Crypto Agency (BSSN). Through regulations, such as BSSN Regulation No. 4 of 2021 and No. 8 of 2024, BSSN provides robust security management and audit standards, ensuring that every innovation is subject to measurable national security governance (Baso et al., 2024). The existence of clear and structured regulations will help build public and business sector trust in adopting blockchain technology (K. S., 2023).

The most significant development that refined the legal framework was the enactment of Government Regulation No. 28 of 2025 concerning the Implementation of Risk-Based Business Licensing. This regulation explicitly recognizes "blockchain technology development activities" as official business activities within the Electronic Systems and Transactions Sector. This formal recognition marks a significant shift, as blockchain is no longer viewed merely as a promising technology but as a state-regulated business sector. Furthermore, through this Government Regulation, the government establishes structured administrative sanctions, ranging from written warnings to revocation of Business Licensing (PB). By regulating these activities within the PBBR system, the government provides clearer legal certainty for innovators and business actors, while also creating an integrated oversight framework equipped with structured administrative sanctions. This implicitly directs that the most likely implementation model is a permissioned blockchain, where innovation can develop within the corridors of state oversight, rather than as an anonymous system operating outside of government control.

Table 2. Blockchain Regulation Matrix in Indonesia

Regulation	Publishing Agency	Main Substance	Status
Law No. 4 of 2023 (P2SK Law)	House of Representatives/ President of the Republic of Indonesia	Transferring oversight of crypto assets from the Commodity Futures Trading Regulatory Agency to the Financial Services Authority and Bank Indonesia; classifying crypto as a Digital Financial Asset.	Valid
Government Regulation No. 28 of 2025	President of the Republic of Indonesia	Legal protection for the development and widespread use of blockchain technology, including in the public sector and MSMEs.	Valid
Financial Services Authority Regulation No. 27 of 2024	Financial Services Authority (OJK)	Technical implementation rules for supervision of Digital Financial Asset trading, including licensing, governance, and consumer protection.	Valid
PBI No. 18/40/PBI/2016	Bank Indonesia (BI)	Regulates the implementation of payment transaction processing; forms the basis for prohibiting the use of virtual currency as a means of payment.	Valid
Government Regulation No. 71 of 2019 & Minister of Communication and Information Regulation No. 5 of 2020	Government & Ministry of Communication and Digital	Require all digital platforms, including blockchain-based ones, to register as Electronic System Providers (PSE).	Valid
Presidential Decree No. 53 of 2017 (amended by Presidential Decree No. 28 of 2021)	President of the Republic of Indonesia	Establish the National Cyber and Crypto Agency (BSSN) as the main national cyber security and cryptography agency.	Valid

Source: *Database of laws and regulations of each agency*

Despite the legal foundation, blockchain implementation faces two fundamental challenges stemming from existing regulations. The first and most crucial challenge stems from Law No. 27 of 2022 concerning Personal Data Protection (PDP Law).

Blockchain's immutable nature directly conflicts with the data subject's right to be forgotten, as mandated by Article 9 of the PDP Law, creating a significant technical-legal conflict (Jung, 2022). This is further exacerbated by the need to comply with data protection regulations, where research shows the importance of privacy-first technology in blockchain-based systems (Mustafa et al., 2025). The second challenge is architectural, stemming from Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System (SPBE) and its derivatives. The SPBE's mandate to centralize data through the National Data Center (PDN) presents a philosophical paradox with the essence of blockchain, which offers decentralization (Kalla et al., 2020).

This regulatory dynamic is further emphasized by the enactment of Government Regulation No. 28 of 2025, which, while formally recognizing blockchain development activities, still places them within a centralized licensing and oversight framework. This indicates that the government supports innovation while remaining within strict control, reinforcing the conflict between the vision of technological decentralization and policy centralization. Research shows that addressing the legal and operational issues surrounding the implementation of blockchain technology in e-government requires a comprehensive framework (Mustafa et al., 2025).

Analysis of sectoral regulations, such as Bappebti's policy of regulating crypto assets as commodities (Bappebti Regulation No. 5 of 2019) and Bank Indonesia's initiative for the Digital Rupiah ("Garuda Project"), shows a very cautious government approach and a tendency to maintain central control (Suretno & Ranggadara, 2022). Thus, it can be concluded that the regulatory framework in Indonesia is leading blockchain adoption toward a "middle ground." The most likely model to succeed is a permission blockchain system with clear governance, implementing privacy-by-design principles to comply with the PDP Law (for example, by storing personal data off-chain) (Suprijandoko, 2020), and fully comply with national cybersecurity standards from BSSN (Akib et al., 2020). The research findings indicate that no single legal framework can be categorized as either a driver or a barrier (Siraz, 2023). Rather, each regulation has dual implications, with some articles providing a foundation that enables innovation, while others create fundamental limitations and challenges that must be navigated. To synthesize and visualize this dualistic dynamic, the findings from the previous regulatory analysis are systematically summarized in a matrix in the following table. This table maps the implications of each major legal framework, both as facilitating and challenging factors for blockchain implementation in the Indonesian government.

Table 3. Synthesis Matrix of Blockchain Regulatory Implications in Indonesia

Regulation	Relevant Key Terms	Implications as a Driver of Blockchain Adoption	Implications as Barriers/Challenges to Blockchain Adoption
Government Regulation No. 28/2025 (PBBR)	**Article 186:** Classifying "blockchain technology development activities" as business activities in the Electronic Systems and Transactions Provision Sector. **Articles 536 and 537:** Regulate administrative sanctions (warnings to revocation of PB) for business actors in this sector.	• Providing Legal Certainty: For the first time, the government has officially recognized and regulated blockchain development as a legitimate business sector. Encouraging Investment: With clear licensing, investment interest in the blockchain technology sector could increase. • Providing a Supervisory Framework: Establishing the basis for formal government oversight of blockchain business activities.	• Potential Increased Administrative Burden: Businesses are now required to comply with Risk-Based Business Licensing (PBBR) requirements, which can increase compliance complexity. • Sanction Risk: Formal sanctions can be a deterrent for innovators or startups that do not fully understand the regulatory framework.
Electronic Information and Transactions Law & Its Amendments	**Article 5 & 6:** Electronic Information/ Documents as legal evidence. - Article 11: Electronic Signatures have legal force.	• Provides a legal basis for transaction records (ledgers) and smart contracts on the blockchain. • Recognizes cryptographic signatures as a legally valid form of agreement.	• Changes to laws that are often reactive to social issues (e.g., hate speech) can create legal uncertainty for decentralized platforms that are difficult to control.

Regulation	Relevant Key Terms	Implications as a Driver of Blockchain Adoption	Implications as Barriers/Challenges to Blockchain Adoption
Law No. 27/2022 (Personal Data Protection Law)	• Data Subject Rights (including the right to rectification and erasure). • Data Controller Obligations (including data minimization). • Cross-border data transfer requirements.	• Encourage the development of privacy-preserving blockchain architectures (e.g., off-chain storage, ZKPs). • Force the adoption of permissioned blockchain models that are more accountable and have clear governance.	• A fundamental conflict between blockchain's immutability and the legally mandated right to data erasure. • The complexity of defining "Data Controller" and "Data Processor" in a decentralized network. • Potential violations of data transfer rules if nodes are distributed globally without equivalent protection mechanisms.
Presidential Regulation on Electronic-Based Government Systems (No. 95/2018 & 132/2022)	• Mandate for an integrated and comprehensive system. • Mandatory integration through the National Data Center (PDN). • Focus on centralized interoperability.	• Promote standardization that can facilitate interoperability between different government blockchain systems in the future. • Provide a basic infrastructure (PDN) that can serve as a physical location for government nodes.	• The architectural and philosophical clash between the highly centralized vision of SPBE and the fundamentally decentralized nature of blockchain hinders the exploration of fully distributed and single-point-of-failure governance models.
National Cyber and Crypto Agency Regulations (No. 4/2021 & 8/2024)	• Information security management obligations (risk-based). • Standards and procedures for periodic SPBE security audits.	• Providing a mature, technology-agnostic governance and audit framework to assess and ensure the security of blockchain systems. • Ensuring technological innovation is balanced with stringent national security standards.	• May increase implementation costs and complexity due to stringent compliance and audit requirements. • Scarcity of human resources (auditors) with dual competencies in E-Government System audits and blockchain-specific security.
Sectoral Regulation (Commodity Futures Trading Regulatory Agency & Bank Indonesia)	• Commodity Futures Trading Regulatory Agency: Crypto assets are classified as commodities. • Bank Indonesia: Exploring Digital Rupiah (CBDC) with controlled DLT.	• Creating legal clarity by separating speculative assets from the realm of legitimate currencies. • Paving the way for DLT innovation in the financial sector in a controlled and regulated manner.	• Demonstrates a very cautious and centralistic approach by the government, which may limit the exploration of the full disruptive potential of purely decentralized technologies.

Source: *Results of data processing by researchers.*

The synthesis matrix in the table above indirectly confirms that blockchain technology adoption in the Indonesian public sector cannot be achieved with a "one-size-fits-all" approach or by importing the technology outright. Attempts to simply replace centralized databases with fully decentralized public blockchains will be doomed to failure, as they directly conflict with various national regulatory pillars, particularly the Personal Data Protection Law and the Presidential Regulation on Electronic-Based Government Systems (SPBE).

Therefore, this regulatory conflict further emphasizes why the permissioned blockchain model is the most realistic 'middle ground.' Unlike public blockchains (such as Bitcoin or Ethereum), which are open, anonymous, and completely decentralized, permissioned blockchains allow only trusted, authorized entities to participate in the network (Hewa et al., 2021). This model allows the government to maintain necessary governance and oversight controls while still leveraging the advantages of blockchain technology, such as limited transparency and resistance to manipulation. Thus, permissioned blockchain bridges the paradox between technological decentralization and policy centralization and enables the application of privacy-by-design principles to comply with the PDP Law. This approach aligns with the spirit of Government Regulation No. 28 of 2025, which places blockchain development within a state-supervised licensing framework, rather than as a technology operating outside government control. Ultimately, the entire system must be designed to be auditable and certified in accordance with the BSSN cybersecurity framework, while leveraging the legality of transactions guaranteed by ITE Law. Without careful alignment between technological innovation and regulatory compliance, blockchain's transformative potential will be difficult to fully realize.

3.2. Division of Authority of Agencies

One fundamental aspect in analyzing technology adoption readiness at the government level is a clear governance structure and division of authority among state institutions. For complex and cross-sectoral technologies like blockchain—which

touch on areas such as technology regulation, business process reform, cybersecurity, and evaluation—a well-defined structure is a prerequisite for preventing overlapping policies and ensuring coordinated implementation (Stephanie et al., 2024). The findings from this research interview identified that the Indonesian government, at least formally, has established a relevant institutional architecture to oversee digital transformation (Wardhana, 2024). In addition, the use of blockchain can improve database security and information transparency, which in turn supports better governance (Maulani et al., 2023). To provide a clear picture of this architecture, the roles and authorities of each key institution are presented in Table 4.

Table 4. Division of Authority of Agencies Related to Blockchain Activities

Activity	Main Agency	Key Legal Basis	Relevant Agencies	Key Notes
Licensing of Crypto Asset Exchanges & Traders	Financial Services Authority (OJK)	POJK No. 27/2024; UU P2SK	Commodity Futures Trading Regulatory Agency, Ministry of Communication and Digital	The Commodity Futures Trading Regulatory Agency plays a role during the transition period. Registration of Electronic System Providers with the Ministry of Communication and Digital is a prerequisite.
Crypto Asset Issuance (ICO/STO)	Financial Services Authority (OJK)	UU P2SK; POJK No. 27/2024	Ministry of Communication and Digital, National Cyber and Crypto Agency	Supervised as a capital market activity. Required to register as an Electronic System Provider and comply with cybersecurity standards.
Use of Crypto for Payments	Bank Indonesia (BI)	UU Mata Uang; PBI No. 18/2016	-	Strictly prohibited. Only Rupiah (including the future Digital Rupiah) is valid as a means of payment.
Non-Financial Blockchain Application Development	(General)	PP No. 28/2025	Ministry of Communication and Digital, National Cyber and Crypto Agency, Sectoral Ministries/Institutions	Supported by the government but required to comply with the regulations of the Electronic System Organizer of the Ministry of Communication and Digital and the security standards of the National Cyber and Crypto Agency.
Online Platform Registration (PSE)	Ministry of Communication and Digital	PP No. 71/2019; Permenkominfo No. 5/2020	-	Mandatory for all digital service providers, including blockchain-based ones.
Cybersecurity and Cryptography Standards	National Cyber and Crypto Agency (BSSN)	Perpres No. 53/2017; Peraturan BSSN terkait	Financial Services Authority, Bank Indonesia, Ministry of Communication and Digital	Setting security standards, conducting audits, and managing national cyber incidents.
Taxation of Crypto Transactions	Ministry of Finance (Directorate General of Taxes)	PMK No. 68/2022	Financial Services Authority, Commodity Futures Trading Regulatory Agency	Value Added Tax and Income Tax are imposed on crypto asset transactions.
Consumer Dispute Resolution	Financial Services Authority (OJK)	UU P2SK; POJK No. 27/2024	-	The Financial Services Authority is the main institution for handling consumer complaints and disputes in the financial services sector.

Source: *Database of regulations for each agency*

Based on the role mapping in the table above, it is clear that the government has built a comprehensive governance foundation. The presence of the Ministry of Communication and Informatics as the technology sector leader, the Ministry of Administrative and Bureaucratic Reform (PAN-RB) as the business process focus, the National Agency for National Security (BSSN) as the information security guardian, and the National Agency for Research and Innovation (BRIN) as the independent evaluator demonstrates that crucial aspects of electronic system implementation have been structurally addressed. This framework theoretically provides a strong foundation for supporting technological innovation in the public sector.

However, the existence of these formal structures alone does not automatically guarantee the smooth adoption of disruptive technologies like blockchain. Other findings in this study suggest that the main challenge lies not in the absence of institutions, but rather in the synergy, mandate strength, and political will to mobilize these institutions simultaneously (Marchenko & Dombrovska, 2023). The effectiveness of this framework depends on the existence of more specific derivative policies and strong political support to ensure each institution can carry out its role harmoniously to achieve national implementation goals. Research shows that the successful integration of blockchain technology in government depends not only on existing infrastructure, but also on support for interoperability between institutions and commitment from stakeholders to drive necessary changes in processes and

policies (Ren, 2023). This shows that synergy between technology, policy, and political support is crucial to maximize the transformational potential offered by blockchain (L. Wang, 2024).

3.3. Blockchain's Fundamental Potential for Indonesia's Public Sector

One of the most significant findings of this study is the stark disconnect regarding the actual implementation of blockchain technology within the Indonesian government. Analysis of the interview data revealed fragmented narratives and polarized views among expert informants. On the one hand, optimistic views claim that several implementation initiatives are already underway and even at the operational stage in several ministries and state-owned enterprises (Calment et al., 2024). This view highlights concrete progress and clear strategic plans in certain sectors. For example, several studies have shown that blockchain technology can improve supply chain management and increase transparency in business processes (Indraprakoso & Haripin, 2023). However, on the other hand, there is skepticism reflecting the challenges in implementing this technology, including issues regarding regulation and synergy between institutions, which often hinder expected progress. Although studies on blockchain security and implementation cover issues related to challenges, as discussed in Munawar et al. (2023), this disconnection creates uncertainty about how and when blockchain technology will be widely integrated into the government sector.

However, on the other hand, there is a counter view that firmly states that effective blockchain adoption has not yet occurred and that existing initiatives are nothing more than pilot projects that have not been tested on a national scale (Y. Xu et al., 2023). This view underscores the low adoption rates and difficulties governments face in adopting new technologies in general (Höhne & Tiberius, 2020). Several studies have noted that many projects are only at the experimental stage, and challenges in integration and the support needed for broader scale remain major obstacles (Y. Wang et al., 2019). This shows that without adequate infrastructure support and a clear policy framework, blockchain's potential cannot be optimized (Bag et al., 2021). To systematically map these crucial differences of view, the key findings from both perspectives are presented in Table 5.

Table 5. Differences in Views Regarding the Status of Blockchain Implementation in Indonesia

View 1: Implemented	View 2: Still in the Pilot Project Stage
The electronic diploma infrastructure at the Ministry of Education, Culture, Research and Technology has been implemented and is blockchain-based.	Many agencies (Ministry of Communication and Digital, banking) have conducted pilot projects and seminars, but none have been implemented in real government.
ID Food (Holding BUMN Pangan) has used blockchain for supply chain management.	The government has not yet effectively adopted blockchain; its current effectiveness remains very low.
There are concrete implementation plans for land certificates (ATR/BPN), e-stamp (Peruri), and Digital Rupiah (Bank Indonesia).	Even simpler technologies like IPv6 have not been effectively implemented, demonstrating the difficulty of adopting new technologies.
DAO (Distributed Autonomous Organization) is referred to as one of the real applications for collective decision automation.	Full crypto usage in the Indonesian government does not exist yet.

Source: *Results of data processing from researchers based on interview findings*

As illustrated in Table 5, the contradiction between these two perspectives is clear and constitutes a central finding of this study. This narrative gap indicates more than just a difference of opinion; it suggests several fundamental problems within the government technology adoption ecosystem. First, it suggests the possible lack of a unified and transparent national roadmap accessible to all stakeholders. As a result, information on implementation progress is fragmented.

Second, this disparity may reflect the existence of "innovation silos," where some ministries or agencies may be moving forward independently, but their successes or trials are not well communicated or integrated into the broader national strategy. Thus, it can be concluded that despite some noteworthy progress, the implementation of blockchain technology in the Indonesian public sector as a whole remains at a very early, fragmented, and strategically immature stage, with little to no impact on the national scale. This narrative gap is an early indication of the fundamental challenges that will be discussed in the following sections.

3.4. Blockchain Adoption Readiness Case Study: QRIS Digital Transformation as the Foundation for National-Scale Technology Adoption

To understand Indonesia's readiness to adopt transformative technologies like blockchain, it is important to analyze case studies of successful large-scale digital technology implementations. In this context, the Quick Response Code Indonesian Standard (QRIS), initiated by Bank Indonesia, serves as a highly relevant precedent. Although QRIS is not fundamentally blockchain technology and operates on a centralized architecture, its successful widespread adoption provides valuable lessons regarding the capacity of Indonesia's digital ecosystem and demonstrates a strong foundation for further innovation. An analysis of QRIS as a proxy for readiness to adopt more complex technologies can be broken down into the benefits achieved and the limitations identified, where blockchain has the potential to offer improvements.

Table 6. Use of QRIS as an Example of Blockchain Adoption in Indonesia

Aspect	The Success of QRIS Architecture (Centralized)	Limitations and Potential Improvements with Blockchain
Interoperability and Standardization	Successfully uniting various Payment Service Providers (PJP) in a single QR code standard.	This success becomes an important model for the implementation of permissioned blockchain in the public sector involving many agencies.
Financial Inclusion	Accelerating financial inclusion by enabling millions of MSMEs to accept digital payments without expensive EDC devices.	Proving the willingness of the public and business actors to adopt new technology if it provides real benefits and is easy to use.
Transaction Efficiency	Reduces reliance on cash, thereby increasing efficiency, security and ease of tracking transactions.	In line with the goal of transparency that blockchain technology inherently offers.
System Dependence	Fully dependent on the infrastructure and policies of Bank Indonesia and the designated switching institutions.	Blockchain Potential: Its distributed nature offers greater resilience and eliminates single points of failure.
Settlement and Reconciliation Process	The fund settlement process between PJPs still goes through traditional banking infrastructure which takes time (T+1 or T+2).	Blockchain Potential: Smart contracts can automate the settlement process to near real-time, reduce costs, and increase liquidity.
Privacy & Data Ownership	Transaction data is centralized in a few large entities, raising questions about privacy and the potential commercialization of data.	Blockchain Potential: Privacy-by-design and Self-Sovereign Identity (SSI) architecture can give data control back to individuals.

Source: *Results of primary and secondary data processing by researchers.*

Thus, the success of QRIS is not an argument to deny the need for blockchain, but rather the opposite; it is empirical validation of the readiness of Indonesia's ecosystem. QRIS has successfully overcome the non-technical challenges that often hinder government digital projects, such as coordination between stakeholders, public education, and adoption by MSMEs. This success proves that Indonesia is capable of executing a national-scale digital transformation project. Therefore, the inherent limitations of QRIS's centralized architecture—such as the risk of a single point of failure and the lack of real-time settlement processes—instead serve as the strongest business and technical justification for moving to the next phase. That phase explores how blockchain's principles of decentralization, cryptographic transparency, and automation through smart contracts can be used to strengthen, secure, and refine the "digital toll road" whose foundation QRIS has successfully built.

3.5. Challenges and Risks of Implementing Blockchain Technology in Indonesian Government

A technology with regulatory compliance, blockchain's transformative potential will be difficult to realize without clarity in governance structures and the division of authority among state institutions. One fundamental aspect in analyzing the readiness for technology adoption at the government level is clarity in governance structures and the division of authority among state institutions. For a complex and cross-sectoral technology like blockchain—which touches on areas such as technology regulation, business process reform, cybersecurity, and evaluation—a well-defined structure is a prerequisite for preventing overlapping policies and ensuring coordinated implementation (Stephanie et al., 2024). The findings from this research interview identified that the Indonesian government, at least formally, has established a relevant institutional architecture to oversee digital transformation (Wardhana, 2024). In addition, the use of blockchain can improve database security and information transparency, which in turn supports better governance (Maulani et al., 2023). To provide a clear picture of this architecture, the roles and authorities of each key institution are presented in Table 7.

Table 7. Challenges and Risks of Implementing Blockchain Technology in the Indonesian Government

Aspect	The Success of QRIS Architecture (Centralized)
Politics and Bureaucracy	Political Will: Identified as the biggest challenge. Blockchain threatens the interests of those in power who are accustomed to opaque systems.
Politics and Bureaucracy	Resistance from "Individuals": There is resistance from individuals who are comfortable "playing" in the loopholes of the current system and feel that their interests are being disturbed.
Politics and Bureaucracy	Leadership Style: Political stability is not enough if the ruling regime is authoritarian or anti-transparency.
Budget & Economy	High Implementation Costs: Development costs can be 5-10 times higher than typical applications, creating resistance.
Budget & Economy	Budget Politics: Efficiency policies and budget cuts make the implementation of new technologies increasingly far from expectations.
Budget & Economy	Difficult to Prove Efficiency: Since there has been no real implementation, it is difficult to calculate efficiency for budget justification.
Social & Human Resources	Mindset Change: Difficulty changing the culture from a personal trust-based system to a technology-based trust system (trustless system).
Social & Human Resources	Low Literacy and Understanding: Blockchain is still considered "alien technology" among governments and the public.
Social & Human Resources	Talent Scarcity: Human resources who master blockchain technology (developers) are still few in Indonesia.
Social & Human Resources	Lack of Public Demand: The public has not actively demanded transparency through this technology, so there is no political pressure.
Technical and Infrastructure	Infrastructure Gap: Stable internet interconnection, a key requirement for blockchain, is not yet evenly distributed across Indonesia.
Technical and Infrastructure	Data Center Fragmentation: Having more than 2,000 data centers spread out increases vulnerability.
Regulations and Laws	Lack of Specific Legal Umbrella: The absence of a law that expressly provides a legal umbrella makes official adoption difficult.
Operational Risk	Human Error Factor: The biggest weakness in cybersecurity is user negligence.

Source: *Results of processing interview findings data by researchers*

The data presented in Table 7 confirms that the challenges facing blockchain adoption in Indonesia are dominated by socio-political and organizational factors. The finding that political will is identified as the biggest obstacle, exacerbated by resistance from individuals and restrictive budget policies, suggests that the root of the problem is fundamental. These challenges are not isolated but form a network of interlocking issues.

For example, a lack of political will directly impacts budgetary policies that discourage high-cost innovation. These budget limitations, in turn, hamper efforts

to improve technical infrastructure and develop human resources (HR). On the other hand, less competent HR will struggle to change mindsets and tend to be resistant to change, ultimately reinforcing leaders' reluctance to commit. Thus, it can be concluded that the barriers to blockchain adoption in Indonesia are not merely technical issues, but rather systemic issues rooted in bureaucratic culture, political dynamics, and the overall ecosystem's readiness.

4. Conclusion

This study argues that the failure of blockchain technology adoption in the Indonesian public sector is not due to technical barriers, but rather to a socio-political and organizational paradox. The article's primary contribution is shifting the discourse from mere technical feasibility to an analysis of fundamental challenges rooted in a lack of political will, bureaucratic resistance, and budgetary politics. Amidst the clash between the vision of technological decentralization and the state's centralization policy (SPBE), and the conflict between blockchain immutabilities and data privacy rights (UU PDP), the only realistic and legally accountable path forward is through an architectural and policy 'middle ground': the implementation of a permissioned blockchain model. This model, as a blockchain with limited access for authorized parties, allows the government to maintain necessary control and oversight (in accordance with the spirit of Government Regulation No. 28 of 2025 and SPBE), while simultaneously complying with the PDP Law through the application of the privacy-by-design principle.

To realize this approach, several strategic initiatives are crucial. Strong institutional synergy is needed between the Ministry of Communication and Informatics, the National Agency for National Development Planning (BSSN), the Ministry of Administrative and Bureaucratic Reform (PAN-RB), and the National Agency for Research and Innovation (BRIN) to address the current weak coordination. Furthermore, the development of an integrated and transparent national roadmap is a prerequisite for eliminating inter-agency "innovation silos" and the resulting fragmented narratives. These efforts must focus on building strong political will as a foundation, overcoming resistance from individuals whose interests are threatened by transparency, and transforming the bureaucratic culture from a system based on personal trust to one based on technology. Nevertheless, this study has several limitations that should be acknowledged. First, as a qualitative study, the findings, based on in-depth interviews with purposively selected informants, provide rich insights but cannot be statistically generalized to represent the entire state apparatus. Second, the analysis of budget constraints is qualitative and does not quantitatively measure potential efficiencies or justify the investment required for large-scale implementation. Third, while recommending a permissioned blockchain model, this study does not design a technical and legal architecture specific to the Indonesian context.

Based on these limitations, future research is strongly recommended to take several strategic directions. Quantitative analysis is needed to measure the impact of blockchain implementation on budget efficiency to provide a strong investment justification for policymakers. Furthermore, future studies should focus on designing and testing permissioned blockchain architecture models that are technically and legally aligned with Indonesia's regulatory ecosystem. Finally, given that bureaucratic resistance is a major obstacle, further study on effective change management strategies to build public and internal support is urgently needed to ensure the long-term success of this digital transformation.

Acknowledgment

The authors express their sincere gratitude to the expert speakers from government, academia, and practitioners for their invaluable support and insights. Their participation and perspectives were fundamental to the completion of this study.

References

Adawiah, R., Kiptiah, M., & Kamariah, N. (2023). Penerapan Penilaian Sikap Siswa pada Pembelajaran Online. *Integralistik, 34*(1), 7–12. https://doi.org/10.15294/integralistik.v34i1.39476

Akhmetbek, Y., & Špaček, D. (2021). Opportunities and Barriers of Using Blockchain in Public Administration: The Case of Real Estate Registration in Kazakhstan. *NISPAcee Journal of Public Administration and Policy, 14*(2), 41–64. https://doi.org/10.2478/nispa-2021-0014

Akib, R., Japri, M., & Kursiswanti, E. T. (2020). Implementasi Pasal 32 Peraturan Pemerintah Republik Indonesia No. 24 Tahun 1997 tentang Pendaftaran atas Tanah di Kota Samarinda (Perkara Perdata Nomor: 27/PDT.G/2016/PN.SMR.). *Abdimas Awang Long: Jurnal Pengabdian Dan Pemberdayaan Masyarakat, 3*(2), 44–51. https://doi.org/10.56301/awal.v3i2.357

Allessie, D., Janssen, M., Ubacht, J., Cunningham, S., & van der Harst, G. (2019). The Consequences of Blockchain Architectures for the Governance of Public Services: A Case Study of the Movement of Excise Goods Under Duty Exemptions. *Information Polity, 24*(4), 487–499. https://doi.org/10.3233/IP-190151

Bag, S., Viktorovich, D. A., Sahu, A. K., & Sahu, A. K. (2021). Barriers to Adoption of Blockchain Technology in Green Supply Chain Management. *Journal of Global Operations and Strategic Sourcing, 14*(1), 104–133. https://doi.org/10.1108/JGOSS-06-2020-0027

Baihaiqi, M. R., Adillah, S. U., & Hasana, D. (2022). Juridical Overview of the Use of Smart Contracts in Indonesia as a Form of Artificial Intelligence Development. *Sultan Agung Notary Law Review, 4*(1), 111–123. https://doi.org/10.30659/sanlar.4.1.111-123

Baso, F., Yusuf, D. U., Djaoe, A. N. M., Iswandi, & Ramadhany, A. (2024). Overview of Smart Contract: Legality and Enforceability. *Dialogia Iuridica, 16*(1), 96–111. https://doi.org/10.28932/di.v16i1.10024

Calment, Victorio, Kosasih, C., Claudya, & Joosten. (2024). Penerapan Teknologi Blockchain dalam Meningkatkan Manajemen Rantai Pasokan Perusahaan. *Nusantara Journal of Multidisciplinary Science, 2*(3), 718–726. https://doi.org/10.60076/njms.v2i4.857

Chen, X., & Lloyd, A. D. (2021). Understanding the Challenges of Blockchain Technology Adoption: Evidence from China's Developing Carbon Markets. *Proceedings of the 54th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2021.685

Chotimah, H. C. (2016). Intergovermental Cooperation Initiative on Sustainable Transportation Management in Jabodetabek. *Jurnal Bina Praja, 8*(1), 121–133. https://doi.org/10.21787/jbp.08.2016.121-133

Daliya, M. S., & Bhandari, A. (2024). The Role of Cybersecurity in Blockchain. *International Journal of Scientific Research in Engineering and Management, 8*(4), 1–5. https://doi.org/10.55041/IJSREM30686

Difrancesco, R. M., Meena, P., & Kumar, G. (2023). How Blockchain Technology Improves Sustainable Supply Chain Processes: A Practical Guide. *Operations Management Research, 16*(2), 620–641. https://doi.org/10.1007/s12063-022-00343-y

Ejairu, E., Mhlongo, N. Z., Odeyemi, O., Nwankwo, E. E., & Odunaiya, O. G. (2024). Blockchain in Global Supply Chains: A Comparative Review of USA and African Practices. *International Journal of Science and Research Archive, 11*(1), 2093–2100. https://doi.org/10.30574/ijsra.2024.11.1.0278

Falcone, E. C., Steelman, Z. R., & Aloysius, J. A. (2021). Understanding Managers' Reactions to Blockchain Technologies in the Supply Chain: The Reliable and Unbiased Software Agent. *Journal of Business Logistics, 42*(1), 25–45. https://doi.org/10.1111/jbl.12263

Firman. (2018). Analisis Data dalam Penelitian Kualitatif. https://www.researchgate.net/publication/328675958

Gong, Y., Zhang, Y., & Alharithi, M. (2022). Supply Chain Finance and Blockchain in Operations Management: A Literature Review. *Sustainability, 14*(20), 13450. https://doi.org/10.3390/su142013450

Hayes, A. (2019). The Socio-Technological Lives of Bitcoin. *Theory, Culture & Society, 36*(4), 49–72. https://doi.org/10.1177/0263276419826218

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges. *Journal of Network and Computer Applications, 177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Höhne, S., & Tiberius, V. (2020). Powered by Blockchain: Forecasting Blockchain Use in the Electricity Market. *International Journal of Energy Sector Management, 14*(6), 1221–1238. https://doi.org/10.1108/IJESM-10-2019-0002

Indraprakoso, D., & Haripin. (2023). Eksplorasi Potensi Penggunaan Blockchain dalam Optimalisasi Manajemen Pelabuhan di Indonesia: Tinjauan Literatur. *Sanskara Manajemen Dan Bisnis, 1*(3), 140–160. https://doi.org/10.58812/smb.v1i03.131

Jung, S. W. (2022). Universal Redactable Blockchain. Journal of Wireless Mobile Networks, *Ubiquitous Computing and Dependable Applications, 13*(4), 81–93. https://doi.org/10.58346/JOWUA.2022.I4.005

K. S., M. (2023). Editorial. *Ushus Journal of Business Management, 22*(4). https://doi.org/10.12725/ujbm.65.0

Kalla, A., Hewa, T., Mishra, R. A., Ylianttila, M., & Liyanage, M. (2020). The Role of Blockchain to Fight Against COVID-19. *IEEE Engineering Management Review, 48*(3), 85–96. https://doi.org/10.1109/EMR.2020.3014052

Lykidis, I., Drosatos, G., & Rantos, K. (2021). The Use of Blockchain Technology in e-Government Services. *Computers, 10*(12), 168. https://doi.org/10.3390/computers10120168

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's Adoption in IoT: The Challenges, and a Way Forward. *Journal of Network and Computer Applications, 125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

Marchenko, V., & Dombrovska, A. (2023). Blockchain Technologies in Digital Economy: Advantages and Challenges. In *The Development of Innovations and Financial Technology in the Digital Economy* (pp. 189–206). Scientific Center of Innovative Research. https://doi.org/10.36690/DIFTDE-2023-189-206

Marlina, L., Anti, N. T., & Ibrahim. (2023). Pelayanan Administrasi di Kantor UPTD Dukcapil Kecamatan Talang Kelapa Kabupaten Banyuasin. *Jurnal Visionary: Penelitian Dan Pengembangan Di Bidang Administrasi Pendidikan, 11*(2), 74–84. https://doi.org/10.33394/vis.v11i2.8770

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi Blockchain pada Sistem Keamanan Informasi. *Jurnal Sosial Teknologi, 3*(2), 99–102. https://doi.org/10.59188/jurnalsostech.v3i2.634

Muhamediyeva, D. T., & Khudoyberdiev, A. N. (2023). Problems of Improving Transactions on the Blockchain. *Matrix Academic International Online Journal of Engineering and Technology, 6*(1), 1–8. https://doi.org/10.21276/MATRIX.2023.6.1.1

Muko, A. (2024). Kajian Smart Contract dalam Perspektif Hukum Positif di Indonesia. *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik, 2*(2), 13–24. https://doi.org/10.59581/doktrin.v2i2.2517

Munawar, Z., Putri, N. I., Iswanto, & Widhiantoro, D. (2023). Analisis Keamanan pada Teknologi Blockchain. *Infotronik: Jurnal Teknologi Informasi Dan Elektronika, 8*(2), 67–79. https://doi.org/10.32897/infotronik.2023.8.2.2062

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-Based Governance Models in E-government: A Comprehensive Framework for Legal, Technical, Ethical and Security Considerations. *International Journal of Law and Management, 67*(1), 37–55. https://doi.org/10.1108/IJLMA-08-2023-0172

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (ASEAN) Regional Forum. *Global Mind, 2*(2), 1–15. https://doi.org/10.53675/jgm.v2i2.89

Ren, Y. (2023). Book Review: The Rise of Blockchains. *International Journal of Knowledge-Based Organizations, 13*(1), 1–6. https://doi.org/10.4018/IJKBO.327451

Saif, A. N. M., Islam, K. M. A., Haque, A., Akhter, H., Rahman, S. M. M., Jafrin, N., Rupa, R. A., & Mostafa, R. (2022). Blockchain Implementation Challenges in Developing Countries: An Evidence-Based Systematic Review and Bibliometric Analysis. *Technology Innovation Management Review, 12*(1/2). https://doi.org/10.22215/timreview/1479

Sinaga, D. N., & Putra, E. V. (2021). Identitas Kolektif dalam Aksi Solidaritas Palestina di Kota Padang. *Jurnal Perspektif: Jurnal Kajian Sosiologi Dan Pendidikan, 4*(4), 887–900. https://doi.org/10.24036/perspektif.v4i4.533

Siraz, R. (2023). Penyusunan Analisa Standar Belanja Kota Pekanbaru. *Portofolio: Jurnal Ekonomi, Bisnis, Manajemen Dan Akuntansi, 20*(1), 56–72. https://doi.org/10.26874/portofolio.v20i1.278

Stephanie, Darianty, R., Ayumi, & Fayola, A. (2024). Tinjauan Literatur terhadap Persiapan dan Tantangan Implementasi Enterprise Architecture di Pemerintahan. *Journal of Data Mining and Information Systems, 2*(2), 97–104. https://doi.org/10.54259/jdmis.v2i2.2958

Suprijandoko, F. (2020). Smart-Pusdiklat: Proyeksi Model Scenario Building and Planning dalam Transformasi Pusdiklat BSSN. *Jurnal Kewidyaiswaraan, 5*(2), 55–61. https://doi.org/10.56971/jwi.v5i2.86

Suretno, M., & Ranggadara, I. (2022). Pengembangan Aplikasi Waste Bank Berbasis Blockchain. *Teknika, 11*(1), 8–13. https://doi.org/10.34148/teknika.v11i1.425

Suwardiyati, R., Widhiyanti, H. N., & Wicaksono, S. (2024). Sah atau Tidak Smart Contract dalam Sistem Blockchain? *Widya Yuridika: Jurnal Hukum, 7*(2), 459–468. https://doi.org/10.31328/wy.v7i2.5156

Tak, P. (2023, April 27). The Critical Determinants of Application of Blockchain Technology in Enhancing Cyber security in the Modern Technology Era. *Proceeding International Conference on Science and Engineering*. https://doi.org/10.52783/cienceng.v11i1.214

Wang, L. (2024). Research on the Impact and Solution Strategies of Blockchain Technology on Data Security and Transparency in Enterprise Digital Transformation. *Advances in Economics, Management and Political Sciences, 103*(1), 156–164. https://doi.org/10.54254/2754-1169/103/20242418

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making Sense of Blockchain Technology: How Will It Transform Supply Chains? *International Journal of Production Economics, 211*, 221–236. https://doi.org/10.1016/j.ijpe.2019.02.002

Wardhana, C. S. (2024). Implementasi Teknologi Blockchain dalam Optimalisasi Keamanan Database Penduduk di Kementerian Dalam Negeri. *Action Research Literate, 8*(4), 915–921. https://doi.org/10.46799/arl.v8i4.305

Wijaksono, S. D., Trianto, R. H., Ikhtiarman, A. F., Amalia, R., & Jannah, F. (2022). Execution of Blockchain in the World of Archive. *Blockchain Frontier Technology, 2*(1), 64–71. https://doi.org/10.34306/bfront.v2i1.115

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *2017 IEEE International Conference on Software Architecture (ICSA)*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Xu, Y., Chong, H.-Y., & Chi, M. (2023). Modelling the Blockchain Adoption Barriers in the AEC Industry. Engineering, *Construction and Architectural Management, 30*(1), 125–153. https://doi.org/10.1108/ECAM-04-2021-0335

Zahra, N., & Amaliyah, N. (2023). Analisis Faktor Rendahnya Literasi Siswa di Kelas 4 SDN Susukan 03 Pagi. *Research and Development Journal of Education (RDJE), 9*(2), 898–905. https://doi.org/10.30998/rdje.v9i2.19454

Zhang, H., Yi, J.-B., & Wang, Q. (2021). Research on the Collaborative Evolution of Blockchain Industry Ecosystems in Terms of Value Co-Creation. *Sustainability, 13*(21), 11567. https://doi.org/10.3390/su132111567

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85