Journal of Central Banking Law and Institutions, Vol. 5 No. 2, 2026, pp. 377 - 400
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
https://doi.org/10.21098/jcli.v5i2.542

LEGAL IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY FOR THE INDONESIAN NATIONAL FINANCIAL SYSTEM AND MONETARY AUTHORITIES

Edmon Makarim
Faculty of Law, Universitas Indonesia
e-mail: edmon@ui.ac.id

Submitted: 12 December 2025 - Last revised: 7 March 2026 - Accepted: 16 April 2026

Abstract

Bank Indonesia faces significant governance challenges as it integrates blockchain technology into the national financial infrastructure. While blockchain offers enhanced transparency and operational integrity, it also raises critical concerns about security, systemic vulnerabilities, and legal accountability. This doctrinal study examines blockchain deployment within the Indonesian financial system, focusing on data protection, technical risks, and the allocation of liability for system failures or breaches. Findings indicate that while decentralised architectures can bolster transactional trust, they are constrained by smart-contract vulnerabilities and interoperability issues. Legally, determining accountability in distributed networks remains problematic, especially where centralised control is absent. Consequently, the study advocates for a comprehensive, adaptive regulatory framework anchored in public institutional authority. Such a framework must align blockchain use with statutory obligations regarding data protection and payment system governance. Grounded in Indonesia's legal structure and international standards, this approach provides a model for jurisdictions seeking to integrate blockchain into state-supervised financial systems.

Keywords: *blockchain, central bank, financial system, legal responsibility, monetary policy, security*

I. INTRODUCTION

The growing deployment of decentralised financial technologies challenges traditional state-centred monetary governance, particularly the statutory mandate of central banks to regulate payment systems and preserve systemic stability. Among these technologies, blockchain has emerged as the most influential innovation, evolving rapidly since its introduction in 2008 as a decentralised payment mechanism operating without state authority.[1] The system was designed to address the problem of double-spending through a proof-of-work (PoW) mechanism, which creates a permanent transaction

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf.

record on a cryptographic chain that is difficult to alter. The core innovation of this system lies in its ability to enable decentralised transaction verification, thereby eliminating reliance on a trusted third party. This mechanism also ensures transaction integrity through consensus based on the computing power contributed by participating nodes.

Nevertheless, the decentralised nature of blockchain gives rise to significant legal issues. When transactions no longer depend on a central authority, questions arise about the allocation of legal responsibility in cases of loss, network attacks, or system failures. In the financial context, blockchain technology has the potential to enhance transaction transparency, efficiency, and security.[2] In the context of blockchain adoption in the financial sector, particularly in payment systems traditionally governed and administered by the state, this concept becomes blurred. This development raises a fundamental legal question regarding the compatibility of decentralised payment technologies with state-based monetary authority and existing legal accountability frameworks.

In Indonesia, the financial sector is overseen by monetary and financial authorities, including Bank Indonesia, the central bank responsible for monetary policy and the payment system; the Financial Services Authority (OJK), the supervisory authority for financial institutions; and the Ministry of Finance, responsible for fiscal policy and state finance functions. This institutional arrangement reflects a centralised governance model in which stability, security, and accountability of the financial system are placed under state authority. The decentralised nature of blockchain, which operates without control by any state or private authority, stands in clear contrast to this model, creating legal uncertainty regarding authority, supervision, and responsibility within the payments system.

Over time, blockchain technology has evolved from a decentralised peer-to-peer payment system introduced by Bitcoin in 2008 into a mature digital financial infrastructure by 2024, with major advances in security, scalability, and functionality. Through developments such as smart contracts, decentralised finance (DeFi), and Central Bank Digital Currency (CBDC), blockchain is positioned as an innovative data-management and transaction system that enables more open, secure, and efficient networks, reducing reliance on central intermediaries. According to CoinMarketCap, the global cryptocurrency market capitalisation reached approximately USD 2.37 trillion by 2024, with nearly 10,000 cryptocurrencies in circulation, indicating rapid growth in blockchain adoption in the financial sector.[3]

---

[2] *Ibid.*

[3] CoinMarketCap, *Global Crypto Market Report* (2024), https://coinmarketcap.com.

However, alongside these developments, blockchain implementation presents significant legal and security challenges. From a technical perspective, vulnerabilities remain, including cyberattacks, manipulation within smart contracts, and risks of data loss due to technical errors. From a legal standpoint, more fundamental issues arise regarding liability and accountability when losses result from system failure or misuse. The absence of a clear central authority raises a critical legal question: whether responsibility for transaction errors, data breaches, or systemic failures within blockchain-based payment systems should rest solely with monetary authorities or be shared with other state institutions whose mandates cover technical, digital, and cybersecurity governance. As highlighted by Tah, Mahula, and Crompvoets, decentralised infrastructure still requires a clearly defined public authority to ensure oversight, risk allocation, and the protection of public interests.[4] This concern is consistent with the International Monetary Fund's position, which emphasises the growing systemic implications of crypto assets and blockchain-based financial infrastructure while balancing innovation with financial stability and consumer protection. This perspective reinforces the view that decentralised payment technologies cannot operate in a legal vacuum. That state responsibility remains central, particularly where systemic risk and the public interest are implicated.[5]

This issue highlights the potential limits of assigning accountability exclusively to monetary authorities, whose primary functions lie in monetary stability and payment system oversight. It raises the question of whether ministries and agencies with technical expertise and regulatory authority over information technology and digital infrastructure should also bear responsibility within a coordinated governance framework.

Against this background, the core issue addressed in this paper concerns how decentralised blockchain-based payment systems can be reconciled with centralised monetary authority and legal responsibility regimes in Indonesia's financial system. This paper examines whether existing legal and regulatory frameworks are adequate to address issues of authority, supervision, and liability arising from the adoption of blockchain in payment systems and explores possible legal approaches to bridge this structural tension.

Scholars have previously examined blockchain from various legal and technological perspectives, particularly concerning its recognition, contractual validity, and regulatory challenges. For instance, Nur Aisah et al. analyse the

---

[4] Evrim Tan et al., "Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management," *Government Information Quarterly* 39, no. 1 (2022): 101625, https://doi.org/10.1016/j.giq.2021.101625

[5] Parma Bains et al., *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets*, IMF Fintech Note No. 2022/007 (International Monetary Fund, September 2022), 10–15, https://www.imf.org/-/media/files/publications/ftn063/2022/english/ftnea2022007.pdf

legal implications of blockchain within the Indonesian legal system, focusing primarily on legal recognition, the validity of smart contracts, and evidentiary aspects.[6] Similarly, Gesa Bimantara examines blockchain from a normative legal standpoint, emphasising its regulatory status and compatibility with existing legal doctrines.[7] Zhang Huang further explores the relationship between blockchain technology and central bank digital currency, identifying functional requirements and technical challenges for CBDC design.[8] In contrast, this article shifts the analytical focus from technological validation to institutional monetary governance, framing blockchain as a governance restructuring phenomenon that affects central banking authority and state accountability.

By combining doctrinal analysis with a micro-comparative approach, this study seeks not only to clarify normative compatibility between blockchain-based infrastructures and existing legal frameworks but also to assess their institutional implications for central bank governance. In particular, the analysis highlights how regulatory design choices may affect monetary sovereignty, systemic risk management, and the operational integrity of national payment systems. The findings, therefore, provide conceptual guidance for monetary authorities in designing blockchain-related regulation within a state-centred financial governance architecture.

II. BLOCKCHAIN IN FINANCIAL SYSTEMS

The development of blockchain technology has undergone significant improvements in security and scalability. From its introduction in 2008 to 2024, blockchain has undergone major developments in its technical architecture and cryptographic algorithms. Since the publication of Bitcoin's white paper in 2008, blockchain has evolved from a decentralised peer-to-peer payment system into a broader financial infrastructure. Starting with Bitcoin's launch in 2009, followed by the emergence of alternative cryptocurrencies, and then by the introduction of smart contracts through Ethereum in 2014–2015, blockchain has expanded from simple transactions to programmable financial applications. After 2016, financial use cases grew rapidly through initial coin offerings (ICOs), the rise of decentralised finance (DeFi), and the development of central bank digital currencies (CBDCs), alongside increasing

[6] Rimal Mahdani and Dara A. Soufyan, "Blockchain and AI in Combating Financial Corruption: A Systematic Literature Review," *Journal of Central Banking Law and Institutions* 5, no. 1 (2026): 125–152.

[7] Gesa Bimantara et al., "Legal Analysis of Bitcoin Ownership as a Medium of Exchange in the Digital Financial System," in Hakamain*: Journal of Sharia and Law Studies* 4, no.1 (2021): 64-77, https://doi.org/10.57255/hakamain.v4i1.1358.

[8] Tao Zhang and Zhigang Huang, "Blockchain and Central Bank Digital Currency," *ICT Express* 8, no. 2 (2022): 264-70, https://doi.org/10.1016/j.icte.2021.09.014.

institutional and regulatory attention. By 2024, blockchain had matured into a key framework for digital finance, reshaping payment systems, financial intermediation, and monetary innovation. This evolution is further illustrated in Table 1, which presents the use of Ethereum-based blockchains in strategic sectors, as summarised by Roman Pavlov.[9] This technological evolution is legally significant, as the increasing complexity and institutional adoption of blockchain-based systems directly affect the allocation of authority, regulatory oversight, and liability within state-governed payment systems.

Table 1.
Ethereum as a catalyst for the transformation of management in the digital economy: from theory to practice[10]

No.	Sphere	Application example	Description
1	Banking	JPM Coin	Digital currency developed by JP Morgan to enable instant payments among institutional clients, built on the bank's proprietary blockchain platform leveraging Ethereum-based technology.
2	DeFi	Uniswap	An Ethereum-based token exchange platform that operates using an automated market maker model without intermediaries.
3	Insurance	Etherisc	A decentralised insurance platform that utilises smart contracts to automate claims processing and payouts.
4	Virtual worlds and real estate	Decentraland	A blockchain-based virtual reality platform where users can create, explore, and monetise digital content and applications.
5	Crowdfunding	Gitcoin	An Ethereum-based platform designed to support open funding for Web3 research and development projects.
6	Energy	Energy Web Foundation	An initiative that applies Ethereum technology to develop decentralised solutions within the energy sector.
7	Art and digital assets	OpenSea	The largest decentralised marketplace for trading NFTs and other Ethereum-based crypto assets.
8	Healthcare	Solve Care	An Ethereum-based platform that facilitates healthcare coordination, payment systems, and secure data exchange among patients, providers, and insurers.
9	Education	Ethereum Education Alliance	An initiative aimed at providing educational programs and resources related to Ethereum and blockchain technology.
10	Gaming industry	Axie Infinity	An Ethereum-based game featuring a play to earn model, allowing players to earn cryptocurrency through gameplay.

[9] Roman Pavlov et al., "Blockchain as a Management Technology: Institutionalization of Crypto-Assets and Transformation of Entrepreneurial Models Using the Example of Ethereum," *Financial and Credit Activity: Problems of Theory and Practice* 6, no. 59 (2024): 157–58.

[10] Roman Pavlov, et.al, "Blockchain as a Management"

In the context of payment and financial transaction systems, blockchain is defined as a chain of digital signatures, in which each asset owner transfers an "electronic coin" by signing the hash of the previous transaction and appending the public key of the next recipient. Holloway argued that blockchain promises significant transformation in the global financial system through increased efficiency, security, and transparency. The integration of this technology into financial systems has attracted the attention of academics and practitioners, with the potential to redefine how financial transactions are conducted and spark innovations.[11] The mechanism for transferring electronic coins by signing prior transaction hashes and attaching the recipient's public key allows the recipient to verify ownership through a continuous chain of signatures linked to all previous transactions.[12]

However, a fundamental issue with this process is the potential for double-spending, in which the same "coin" is used by its previous owner to transfer value to multiple parties. Conventional transaction systems typically rely on a central authority—such as banks, financial institutions, or government bodies—to verify each transaction and prevent double-spending. Yet this approach creates complete dependence on a centralised third party.

To address this, a system is needed that enables all network participants to know the transaction sequence without relying on a central authority. Blockchain provides a solution through a consensus mechanism that distributes verification across nodes,[13] enabling transactions to be validated based on the agreed order of receipt as confirmed by the majority of the network. In the context of blockchain, a node refers to a computer or device that forms part of a peer-to-peer network and is responsible for executing the system protocol, maintaining copies of transaction records, and participating in the consensus process. Each node receives and broadcasts new transactions, aggregates them into blocks, verifies transaction validity through proof-of-work or other consensus mechanisms, and subsequently propagates newly validated blocks across the network. Nodes also determine which block is considered valid by following the longest-chain rule, which treats the authoritative transaction ledger as the authoritative transaction ledger. Through these functions, nodes serve as the fundamental pillars for maintaining security, transparency, and data synchronisation across the blockchain network, thereby preventing abuses such as double-spending and ensuring the reliability of digital payment systems. This model ensures transaction authenticity, reduces reliance on third parties, and enhances the security and transparency of digital payment systems.

[11] Samuel Holloway, "Examining the Adoption of Blockchain Technology in Financial Information Systems", *SSRN Electronic Journal,* (January 2025), 9

[12] Nakamoto, *Bitcoin.*

[13] Nakamoto, *Bitcoin.*

In payment and financial applications, blockchain introduces a concept called Simplified Payment Verification (SPV), which enables faster, more efficient payment verification without running a full node on the blockchain network. SPV works by allowing users to store only the block headers of the longest proof-of-work chain, which network nodes can verify to ensure authenticity.

In blockchain systems, a Merkle branch is part of a data structure known as a Merkle tree, a binary tree constructed from a series of hashed transactions within a block. Each transaction in the block is hashed and then combined pairwise until a single root hash, known as the Merkle root, is produced. A Merkle branch refers to the sequence of hashes that links an individual transaction to the Merkle root. Its function is to prove that a specific transaction is indeed recorded within a block without requiring verification of the block's entire contents. This mechanism enables more efficient verification processes, particularly in SPV, where users only need to examine the transaction's linkage through the Merkle branch to confirm its validity. Merkle branches play a crucial role in preserving transaction data integrity, enhancing verification efficiency, and ensuring transparency across blockchain systems, thereby constituting a fundamental instrument for guaranteeing the security and validity of distributed ledger technology. Using a Merkle branch structure, users can link a specific transaction to a time-stamped block without verifying all transactions directly. Although users cannot perform full transaction checks, the linkage between the transaction and the block indicates that the network has accepted it. The addition of subsequent blocks serves as further confirmation. For this reason, SPV offers highly efficient payment verification while maintaining security through the blockchain's consensus mechanism.[14] Despite blockchain's strong resistance to manipulation, security concerns remain—particularly for high-risk financial transactions. To strengthen security in digitalisation and blockchain use, a concept called smart contracts[15] is used. Smart contracts represent a significant innovation in blockchain technology, functioning as computerised transaction protocols that automatically execute the terms of an agreement. The concept was first introduced by Nick Szabo in 1994 to secure, enforce, and facilitate the performance of contractual arrangements recorded between individuals or organisations. Unlike conventional contracts, smart contracts are dynamic, as they can transmit information, perform computations, and even execute predetermined decisions without human intervention. By virtue of these characteristics, smart contracts reduce reliance on trusted intermediaries, minimise the risk of both intentional and unintentional errors,

[14] *Ibid.*

[15] *Ibid.*

and mitigate fraud, dispute resolution costs, and other transaction-related expenses. More broadly, the design of smart contracts seeks to operationalise common contractual provisions—such as payment conditions, guarantees, confidentiality obligations, and enforcement mechanisms—more efficiently than traditional legal processes. Accordingly, smart contracts not only introduce a new paradigm for the negotiation and execution of agreements but also provide a technological foundation with the potential to transform the practice of contract law in the digital era.

In modern banking, Blockchain technology has significantly increased efficiency, security, and transparency in financial systems. As a decentralised database operated through a distributed computer network, blockchain replaces centralised systems that were previously the main model for financial data storage and verification.

This development is particularly interesting because in Indonesia, the financial system is fully controlled by the state through Bank Indonesia and the Financial Services Authority (OJK).[16] Blockchain's characteristics enable greater efficiency across banking activities, including payment and settlement systems, trade finance, identity management, regulatory compliance, and asset tokenisation. These applications contribute to a more transparent and secure banking ecosystem.

Another major advantage of blockchain is its ability to record transactions in real time, reducing counterparty risk and lowering transaction costs. Swan emphasises that blockchain-based cross-border payment systems can operate faster and more efficiently than traditional systems while significantly reducing banks' operational costs. Therefore, in both financial digitalisation and public administration, blockchain serves as a strategic foundation for improving efficiency, strengthening security, and enhancing public trust in technology-based systems.[17]

In blockchain systems, all transactions must be publicly disclosed across a distributed network to maintain transparency and prevent misuse. A key challenge lies in maintaining privacy without involving a central authority. This is achieved by preserving anonymity using public keys that do not contain personal identity information. In this way, the public can see that a transaction has occurred (e.g., someone transferring digital assets to another party) without knowing the parties' identities.

This model resembles the transparency of stock exchanges, where transaction times and values are publicly disclosed, but the identities of the parties remain private. As an additional security layer, each transaction uses a

[16] Law No. 23 of 1999 on Bank Indonesia (Republik Indonesia).

[17] Melanie Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly Media, 2015).

recommended new key pair to prevent linkages between different transactions. However, this system is not entirely risk-free; in multi-input transactions, ownership can still be identified if one key becomes publicly known, exposing other related transactions.

In legal and technological research, blockchain is viewed as a tamper-proof public records repository that can store and execute various administrative, legal, and economic instructions automatically. Its applications extend beyond financial transaction records to include legal documents, contracts, asset certificates, and public administration systems.

In the financial sector, distributed ledger technologies such as blockchain are valued for their ability to improve the security, efficiency, and transparency of global financial systems. Blockchain facilitates more transparent and secure business networks with standardised operational models, efficient procedures, and lower transaction costs.[18]

Information technology development is now a key determinant of the competitiveness of modern financial institutions. Institutions that fail to adopt digital technology risk losing customers, facing operational inefficiencies, and falling behind in global competition. Financial Technology (FinTech) has become essential in modern finance, with applications in insurance, internet banking, electronic payments, and peer-to-peer lending. As argued by Petrovska, in the era of global digital transformation, financial institutions worldwide are integrating digital innovations into their business strategies to maintain a competitive advantage.[19]

Blockchain shares similarities with innovations under the broader FinTech umbrella. FinTech encompasses technologies such as Regulatory Technology (RegTech) for regulatory compliance, Supervisory Tech (SupTech) for supervisory data analytics, Big Data and Smart Data for predictive analytics, and Distributed Ledger Technology (DLT), such as blockchain, for secure, transparent transaction records. Other technologies, such as Artificial Intelligence (AI), machine learning, open Application Programming Interfaces (APIs), and mobile technologies, would enhance automation, decision-making, and customer experience. Thus, FinTech adoption represents not only technological transformation but also structural change toward a more adaptive, inclusive, and sustainable digital financial ecosystem.[20]

---

[18] Marcella Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," *Journal of Governance & Regulation* 6, no. 1 (2017): 46, https://doi.org/10.22495/jgr_v6_i1_p5.

[19] Zoriana S. Pestovska, "(R)evoliutsiia Bankinhu: Dyskusii ta Perspektyvy [(P)Еволюція Банкінгу: Дискусії та Перспективи," *Academy Review [Пестовська]* 1, no. 54 (2021): 37–47, https://doi.org/10.32342/2074-5354-2021-1-54-4

[20] Olena Lytvyn et al., "Integration of Digital Means in the Financial Sphere: The Potential of Cloud Computing, Blockchain, Big Data and AI," *Financial and Credit Activity: Problems of Theory and Practice* 1, no. 54 (2024): 131-142. 10.55643/fcaptp.1.54.2024.4257.

Digital technology integration in finance has the potential to transform and improve financial services. A key component of this transformation is cloud computing, which enables large-scale data storage and processing with high scalability and availability. Blockchain, as a distributed ledger technology, strengthens transaction security and reliability by reducing the risk of manipulation and fraud while lowering operational and intermediary costs. It also improves internal audit efficiency. Meanwhile, Big Data allows institutions to analyse market trends, assess investment risks, and optimise asset management through data-driven decision-making.

AI also contributes to automation by streamlining processes such as credit scoring, risk analysis, and customer service. AI can detect anomalies and potential fraud early, increasing the reliability of digital financial systems. Nevertheless, modern financial technologies like blockchain, Big Data, and AI pose challenges, including increased risk of data breaches, a lack of unified blockchain regulations, and global disparities in adoption rates. Additionally, unclear regulations can hinder innovation and create legal uncertainty. Therefore, successful digital transformation in finance requires a holistic approach that includes strengthening data security, regulatory standardisation, and international cooperation.

Blockchain enables the integration of digital instruments such as smart contracts, which self-execute based on cryptographic code without third-party involvement; multi-signature transactions, which require approval from multiple parties to enhance transaction security; and smart properties, which digitally represent ownership of tangible or intangible assets and can be tracked on blockchain networks.[21]

A blockchain-based society imagines a social structure without traditional state institutions, driven entirely by algorithms and smart contracts. Within this system, entities such as Decentralised Autonomous Organisations (DAOs) operate automatically, guided by algorithms and market rules, to meet collective needs without third-party intervention.[22] Individuals no longer depend on central authorities; instead, they organise themselves through consensus processes embedded in digital protocols. DAOs can manage resource distribution, maintain digital platforms, and coordinate social services through crowdfunding. Thus, a blockchain society reflects a shift toward a pre-sovereignty condition, where legitimacy is derived not from the state but from algorithmic mechanisms agreed upon by the global digital community.

[21] Atzori, "Blockchain Technology."

[22] Yash Chhunchha, "Revolutionizing Financial Institutions: The Influence of Blockchain Technology in the Banking Sector in California" (PhD diss., Westcliff University, 2025), 20–22.

The use of blockchain in decentralising public services and government administration has sparked academic debates about the extent to which it can replace state archives, notaries, and traditional administrative institutions. Swan argues that blockchain is a superior distributed ledger: efficient, transparent, irreversible, low-cost, and resistant to censorship.[23]

These advantages create opportunities to apply blockchain in government governance, especially to enhance accountability and efficiency. However, decentralising government services through open, unauthorised blockchain systems also brings significant risks related to regulatory uncertainty, system stability, and legal liability.

In the context of privacy protection, particularly in land administration, privacy is crucial for safeguarding ownership data while ensuring transparency in land rights transfers. Blockchain enables transparent recording of transactions without compromising privacy by relying on cryptography and encrypted digital identities. Thus, data security and privacy protection in blockchain implementations must align with the principles of Indonesia's Personal Data Protection Law (the PDP Law) to balance public transparency with individual privacy rights.[24]

Although blockchain initially developed alongside cryptocurrencies, it has now evolved beyond economic functions and become a foundational architecture for various financial and non-financial applications. Its decentralised database features, namely, immutability, non-repudiation, integrity, transparency, and user equality, have led to diverse blockchain models and architectures. However, distributed ledger technologies still face challenges, particularly scalability, flexibility, and governance, which require deeper study within the context of public policy and administration. One of the challenges to blockchain adoption in the financial sector is the absence of a standard implementation framework and a global consensus on regulatory practices.[25] The early stages of blockchain regulatory frameworks across jurisdictions, ranging from a neutral stance by entities such as the Bank of England to more positive assessments by the IMF and the World Bank of distributed ledgers, highlight a fragmented global approach.[26] This regulatory fragmentation, coupled with the inherent complexity of integrating decentralised solutions into established legacy financial infrastructure, presents significant barriers to widespread adoption and interoperability. However, integrating blockchain into existing

[23] Swan, *Blockchain: Blueprint*.

[24] Law No. 27 of 2022 on Personal Data Protection (Republik Indonesia).

[25] Samuel Holloway, "Examining the Adoption", 2

[26] Javier Sebastian Cermeno, *Bitcoin and Its Potential Impact on the Financial System* (Madrid: BBVA Research, December 2016), 2, https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf

financial systems presents significant technical challenges, including ensuring interoperability with legacy infrastructure, addressing scalability limitations, managing the high energy consumption of certain consensus mechanisms, and developing robust security protocols to mitigate cyber threats. Furthermore, the inherent complexity of blockchain systems requires specialised expertise for effective implementation and maintenance, which can hinder adoption by many financial institutions. These challenges collectively complicate seamless integration and underscore the need not only for continued technological advancement but also for clearer regulatory frameworks to realise blockchain's transformative potential in the financial ecosystem fully.[27]

In public administration, a key challenge for policymakers is determining the extent to which blockchain is suitable as the backbone for future public service systems, including registration, archival governance, and administrative services.

III. LEGAL AND SECURITY ISSUES IN BLOCKCHAIN ADOPTION

Referring back to Satoshi Nakamoto's white paper, blockchain relies on a decentralised verification model that prevents unauthorised changes to recorded data. In the context of public administration and digital governance, this approach can strengthen data integrity, reduce bureaucratic inefficiencies, and enhance transparency, provided that its application remains consistent with statutory obligations and regulatory safeguards. However, the immutable nature of blockchain, while beneficial for data integrity, also poses privacy challenges, particularly regarding data deletion or modification.[28] This built-in immutability, combined with the distributed ledger system, requires careful consideration of privacy and data protection rules that ensure rights such as data erasure and data portability.

In Indonesia, the implementation of digital systems must comply with a comprehensive set of statutory and regulatory obligations, particularly those related to the processing of personal or sensitive data. The PDP Law requires data controllers and processors to safeguard the security, confidentiality, accuracy, and integrity of personal data through adequate technical and organisational measures. These measures are not only aimed at preventing unauthorised access, disclosure, alteration, or destruction of personal data, but also ensuring that data remains accurate, up-to-date, and processed in a lawful

[27] Samuel Holloway, "Examining the Adoption", 4-17

[28] Luminita Movanu, "Blockchain for an Efficient Public Administration". *Perspective Politice 16*, (January, 2023). pg. 5 https://doi.org/10.25019/perspol/23.16.0.13

and accountable manner.[29] In this context, data controllers and processors are required to adopt a risk-based approach that takes into account the nature, scope, and potential impact of data processing activities. Although the PDP Law does not specifically address blockchain architectures, the obligations under Articles 29, 35, and 36 apply to all forms of digital data processing systems by virtue of their technology-neutral language. Neutral technology is a regulatory approach that avoids favouring or discriminating against specific technologies, ensuring that legal frameworks remain applicable even as technological advancement emerges.[30] These principles are reflected in Article 3 of Indonesia's Law on Electronic Information and Transactions (the ITE Law), which sets out the fundamental principles governing the use of electronic systems in Indonesia. In parallel, the ITE Law mandates electronic system providers to apply risk-based security standards, maintain resilient infrastructure and backup mechanisms, and ensure data localisation for categories of strategic data. These obligations extend to blockchain applications used in administrative or financial services.[31] These legal requirements mean that blockchain must be implemented carefully in Indonesian public administration, so that its immutable and transparent nature remains aligned with data protection and system security rules.

Complementing these statutes, the Government Regulation on Electronic Systems and Transactions (the PSTE Regulation) imposes requirements for system reliability, security, and operational continuity, including maintaining audit trails and protecting electronic information from loss, alteration, or manipulation, so that electronic transactions remain verifiable and legally accountable.[32] Taken together, this framework requires electronic systems providers to ensure lawful and minimal data processing, maintain continuous and reliable system operations, prevent unauthorised access, and uphold clear accountability in the event of system failures, data leaks, or security breaches. For instance, Articles 20 and 35 of the PDP Law require controllers and processors to implement organisational and technical measures to secure personal data. These include encryption, access restrictions, logging, and risk mitigation procedures. Meanwhile, Article 14 of the PSTE Regulation mandates electronic system providers to maintain system availability, confidentiality, integrity, and authenticity.

---

[29] Law No. 27 of 2022.

[30] Alonel Hugo, "Private Blockchain-Based Procurement and Asset Management System with QR Code." *SSRN Electronic Journal,* (January, 2024), 8 https://doi.org/10.2139/ssrn.4918938

[31] Law No. 11 of 2008 on Electronic Information and Transactions (Republik Indonesia), Arts. 15 and 16.

[32] Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (Republik Indonesia).

When applied to blockchain, these obligations raise several practical questions: How should data correction rights be implemented on immutable ledgers? Who bears responsibility when decentralised nodes operate across jurisdictions? And how should governance be structured when no single entity has full operational control?

To address these concerns, many countries have adopted hybrid models by combining blockchain's transparency with administrative controls and off-chain governance mechanisms. Countries such as Estonia and Singapore have integrated blockchain for specific government functions, leveraging its security and transparency benefits while designing regulatory and legal frameworks that accommodate its unique characteristics, particularly regarding data immutability and distributed consensus.[33] Indonesia may require similar approaches to ensure that blockchain-based public systems remain compliant with statutory duties while leveraging the technology's benefits.

Technically, blockchain systems apply cryptographic hashing, decentralised consensus, and multi-node validation. These features make them resistant to tampering but do not eliminate the possibility of failure. Security risks remain, including cyberattacks, smart contract vulnerabilities, human error, and technical malfunctions. Therefore, electronic system providers remain legally obligated to conduct risk assessments, maintain audit logs, and prepare incident response procedures, as required by Indonesian regulations.

In the medical sector, for example, blockchain can support confidentiality and data integrity, but it must still comply with statutory health data protections. Similar principles apply to land administration, financial services, and national digital identity systems. Therefore, implementing blockchain technology in these critical sectors requires a careful regulatory framework that balances the inherent advantages of decentralisation and resistance to change with existing legal requirements for data governance and data subject rights.

While blockchain technology promises increased efficiency, transparency, and trust within digital ecosystems, its adoption must be supported by clear governance structures, regulatory compliance, accountability frameworks, and robust technical safeguards aligned with national legal and institutional standards. Therefore, the main challenge is not just integrating blockchain into existing financial or administrative systems, but ensuring that such deployment fully complies with legal obligations regarding data protection, system reliability, operational continuity, and user rights. In this context, blockchain

[33] Diky Pratama Putra and Pujiyono Suwadi, "The Legal and System Security hurdles in Implementing Electronic-Based Government System at the Department Population and Civil Registration in Indonesia." *Advances in Social Sciences, Education and Humanities Research, Proceedings of the International Conference on Cultural Policy and Sustainable Development,* (2024), 612

implementation is as much a matter of regulatory and institutional design as it is of technological innovation, requiring careful calibration to avoid legal gaps, operational risks, and unintended systemic vulnerabilities.

IV. MONETARY AUTHORITIES AND THE GOVERNANCE OF BLOCKCHAIN-BASED FINANCIAL INFRASTRUCTURE

The International Telecommunication Union (ITU) underscores that financial inclusion in digital financial services is not merely a matter of technological adoption but rather the result of an institutional governance framework involving multiple, interdependent regulators. In this context, effective coordination among financial regulators, telecommunications authorities, and competition regulators constitutes a foundational prerequisite for inclusive digital financial access. Regulatory coherence across these sectors shapes the structural conditions under which digital financial infrastructures operate. [34] Within this broader governance architecture, this article focuses specifically on the role of monetary authorities as key institutional actors in the oversight and governance of blockchain-based financial infrastructure.

Monetary authorities occupy a central position within this multi-layered regulatory ecosystem, as they exercise both policy-making and infrastructural oversight functions that directly affect the integrity of digital financial systems.[35] As custodians of monetary stability and systemic resilience, monetary authorities are tasked with ensuring that the adoption of DLT doesn't fragment the monetary system or weaken the reliability of payment operations.[36] This responsibility necessitates a governance framework that goes beyond ex post supervision to encompass the design and operational governance of blockchain-based infrastructure.[37] Such a framework must balance innovation and robust oversight, addressing issues of technical interoperability, cybersecurity, data governance, and the allocation of responsibilities and liabilities among participating actors.[38] In this respect, the governance of blockchain-based financial infrastructure represents not merely a technological adjustment but an extension of monetary authority into new forms of digital value and settlement infrastructure.[39]

---

[34] International Telecommunication Union, *Digital Financial Services: Regulating for Financial Inclusion–an ICT Perspective*, (ITU, 2016), 53.

[35] Bank for International Settlements, "The Next-Generation Monetary and Financial System," in *BIS Annual Economic Report* (Bank for International Settlements, 2025): 81. https://www.bis.org/publ/arpdf/ar2025e3.pdf.

[36] Bank for International Settlements, "The Next-Generation," 80-81.

[37] *Ibid,* 82.

[38] *Ibid,* 81-2.

[39] *Ibid,* 82.

This necessitates a comprehensive analysis of their institutional capacity and readiness to integrate such innovations, moving beyond a purely technological perspective to encompass regulatory, normative, and cognitive dimensions of preparedness.[40] This perspective emphasises that the successful implementation of blockchain-based financial infrastructure is closely related to institutional quality, which encompasses a robust governance framework and an inclusive financial system.[41] Indeed, nations with superior institutional quality and strong regulatory frameworks are more likely to successfully adopt CBDC, indicating that regulatory alignment is more important than mere technological factors for such initiatives. Moreover, integrating distributed ledger technology into the financial system requires central banks to develop sophisticated governance structures that accommodate the inherent complexities of decentralised networks while upholding monetary sovereignty and financial stability.[42] This evolving role often entails navigating diverse design options for CBDC and adapting payment systems to disruptive transformations. Such governance frameworks must extend beyond initial codification to encompass ongoing adjudication and conflict resolution within these decentralised systems, ensuring comprehensive oversight.[43]

The institutional role is reflected in Bank Indonesia's statutory mandate under the Bank Indonesia Act, which entrusts the central bank with formulating and implementing monetary policy, regulating and safeguarding the national payment system, and regulating and supervising banking institutions. When blockchain technology is integrated into payment system infrastructure, these mandates imply an expanded governance role for Bank Indonesia, including its qualification as an electronic system provider under the Indonesian Electronic Information and Transactions Law. Consequently, Bank Indonesia bears legal and institutional responsibility for ensuring that blockchain-based payment infrastructure operates securely, reliably, and accountably, and can function continuously and properly.[44] This encompasses compliance with legal, technical, and governance standards to preserve transactional integrity, protect users, and maintain overall systemic stability.

---

[40] Ioannis Tsouris, Georgios L. Thanasas, Maria Rigou, "Assessing the European Central Bank's Institutional Capacity Readiness for the Introduction of the Digital Euro" *Journal of Risk and Financial Management* Vol. 19 Issue 2, (February, 2026), https://doi.org/10.3390/jrfm19020148

[41] Pal, et.al., "Innovation on Credit: The Role of Fintech and Institutional Quality in Global Technological Advancements" *Journal of Innovation and Entrepreneurship* Vol. 14 Issue 1, (2025), 5 https://doi.org/10.1186/s13731-025-00568-8

[42] Guo et al., "Cryptocurrencies and Central Bank Digital Currencies in Global Perspective" *Journal of Risk and Financial Management* Vol. 18 Issue 11, (2025) https://doi.org/10.3390/jrfm18110644

[43] Scheltz, et. al. "Blockchain and Regenerative Finance: Charting a Path toward Regeneration." *Frontiers in Blockchain,* (July, 2023), 7 https://doi.org/10.3389/fbloc.2023.1165133

[44] Law No. 11 of 2008.

Beyond these legal and institutional dimensions, the regulatory approach adopted by monetary authorities also produces significant economic consequences for the functioning of blockchain-based financial infrastructures. Different regulatory strategies can influence the efficiency of payment systems, the level of competition within digital financial markets, the expansion of financial inclusion, and the management of systemic risk in increasingly digitised financial ecosystems.[45] Consequently, the governance framework designed by monetary authorities must not only ensure legal compliance and operational reliability but also shape the economic structure and performance of digital financial infrastructures.

From an efficiency perspective, regulatory frameworks that promote interoperability, open standards, and technological neutrality can significantly reduce transaction costs and improve settlement speed in blockchain-based payment systems. Distributed ledger technologies can streamline clearing and settlement processes, reduce reconciliation requirements, and increase transparency in transaction records.[46] However, fragmented regulatory regimes or inconsistent technical standards may generate additional compliance burdens and limit the scalability of blockchain infrastructures across financial markets. In this regard, a technology-neutral regulatory approach maintains regulatory flexibility while enabling innovation. In the Indonesian context, this principle is already reflected in the ITE Law, which recognises technological neutrality as one of the guiding principles for the utilisation of information technology and electronic transactions. The law stipulates that such utilisation shall be conducted in accordance with the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology, thereby allowing innovation to develop without being constrained by preferences for specific technologies.[47]

Regulatory design also plays an important role in shaping competition within digital financial markets. A governance framework that facilitates open access to financial infrastructure may lower barriers to entry for fintech firms and new payment service providers, thereby fostering competitive innovation in financial services. Conversely, regulatory approaches that concentrate infrastructure control within a limited number of institutions may reinforce market dominance by established financial intermediaries or large technology

[45] Tanai Khiaonarong and Terry Goh, "Fintech and Payments Regulation: Analytical Framework" (IMF Working Paper WP/20/75, International Monetary Fund, Washington, D.C., May 2020), 66, https://www.imf.org/-/media/files/publications/wp/2020/english/wpiea2020075-print-pdf.pdf.

[46] Marco Iansiti and Karim R. Lakhani, "The Truth about Blockchain," *Harvard Business Review 95, no. 1* (2017): 118-27. https://hbr.org/2017/01/the-truth-about-blockchain

[47] Law No. 11 of 2008.

platforms.[48] In this context, monetary authorities must carefully calibrate regulatory frameworks to ensure that blockchain-based infrastructure develops as a competitive, interoperable ecosystem rather than a closed or monopolistic system.

At the same time, the integration of blockchain technology into financial infrastructures introduces new forms of systemic risk that require careful regulatory oversight. Despite the efficiency gains that interoperability and open standards may offer in the deployment of financial infrastructure, they simultaneously risk exposing systems operated by monetary authorities to broader systemic vulnerabilities. These risks may arise from technological concentration, cybersecurity vulnerabilities, operational disruptions, or governance uncertainties within distributed networks.[49] Given the potentially severe impact of cyber incidents on financial stability, the European Systemic Risk Board, the Financial Stability Oversight Council, and the Financial Policy Committee have recognised cyber risk as a source of systemic risk.[50] Blockchain-based financial infrastructures, by virtue of their networked and software-dependent architecture, are particularly susceptible to precisely these categories of cyber-induced systemic disruption.

Balancing transparency with the distributed nature of blockchain is crucial, especially regarding regulatory compliance and centralised control. This is a challenge that many experts, such as Udeh[51], Shoetan, Familoni[52], and Koonprasert[53], have been studying. One way to achieve this challenge is by redescribing the technology to fit the state's goals. This is important for reducing the risks that come with the fragmented nature of blockchain governance. We need to make sure that these new infrastructures improve financial security and efficiency, rather than making things worse. As researchers like Shoetan and Familoni have pointed out, this requires careful consideration of potential

---

[48] OECD, *Competition, Fintechs, and Open Banking: An Overview of Recent Developments in Latin America and the Caribbean, OECD Roundtables on Competition* Policy Papers, No. 313 (OECD Publishing, 2024), 12-13. https://doi.org/10.1787/de9fe6b4-en

[49] Basel Committee on Banking Supervision (BCBS), *Prudential Treatment of Cryptoasset Exposures*, (Bank for International Settlements, 2022) https://www.bis.org/bcbs/publ/d545.pdf

[50] International Monetary Fund, *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risk* (Washington DC, IMF, April, 2024), 87, https://www.imf.org/en/publications/gfsr/issues/2024/04/16/global-financial-stability-report-april-2024

[51] Ezekiel Onyekachukwu Udeh, et.al., "The role of Blockchain technology in enhancing transparency and trust in green finance markets", *Finance & Accounting Research Journal,* Vol. 6 Issue 6, June 2024, 836

[52] Philip Olaseni Shoetan, Babajide Tolulope Familoni, "Blockchain's Impact on Financial Security and Efficiency Beyond Cryptocurrency Uses", *International Journal of Management & Entrepreneurship Research,* Vol. 6, Issue 4, April 2024, 1213

[53] Tayo Tunyathon Koonprasert, Shiho Kanada, Natsuki Tsuda, and Edona Reshidi, "Central Bank Digital Currency Adoption: Inclusive Strategies for Intermediaries and Users", *Fintech Notes 2024,* no. 005 (Washington, DC: International Monetary Fund, 2024), https://doi.org/10.5089/9798400289422.063

problems that could arise. For example, private transactions might become less private, and cross-border transactions using foreign digital currencies could disrupt domestic markets.

Another problem that might arise is how geopolitical shocks might affect the international use of blockchain. To navigate these challenges, policymakers need to continually assess their tools and strategies to facilitate the adoption of new digital financial instruments. This means adapting to the unique circumstances of each jurisdiction, as Koonprasert suggested. By taking a strategic approach, we can ensure that blockchain technology contributes to the overall stability of the financial system, rather than creating new problems. This involves being aware of the potential risks and taking steps to mitigate them, while also embracing the opportunities that blockchain presents. As noted by Stiefel, this might involve rethinking how we describe and understand blockchain technology to align it with the state's goals and the financial system's needs. By doing so, we can create a more secure, efficient, and transparent financial system that benefits everyone. The key is to find a balance between the decentralised nature of blockchain and the need for regulatory compliance. This is a complex undertaking, yet it is crucial to ensure that blockchain technology is applied in a manner that enhances financial security and efficiency. Through collaboration and a well-considered strategic approach, the full potential of blockchain can be realised, paving the way for a more resilient and forward-looking financial system.

Nevertheless, the resilience of blockchain networks is also shaped by governance mechanisms embedded within their technological architecture. As explained by Hossein Nabilou, the resilience of blockchain networks largely depends on internal governance mechanisms embedded within their protocol architecture and maintained through distributed consensus processes. Rather than relying on centralised authorities, blockchain systems utilise algorithmic governance structures to validate transactions, coordinate network participation, and maintain the ledger's integrity and continuity.[54] While these mechanisms may enhance operational resilience by distributing authority across multiple actors, they do not eliminate the need for public regulatory oversight, particularly where blockchain infrastructure becomes a systemically relevant component of the financial system. However, the absence of a single controlling entity in distributed networks requires a regulatory design that explicitly attributes legal responsibility to identifiable nodes, operators, or validators, rather than relying on conventional principal–agent frameworks.

[54] Hossein Nabilou, "Bitcoin Governance as a Decentralized Financial Market Infrastructure," *Stanford Journal of Blockchain Law & Policy* 4, no. 2 (2019): 201. https://hdl.handle.net/11245.1/baf416c7-5ed7-4b61-8a22-d70d91336bc1.

This is where monetary and financial authorities are charged with crafting an optimal regulatory design that balances efficiency and risk mitigation.

Ultimately, the successful integration of blockchain-based financial infrastructure by monetary authorities hinges on their ability to cultivate public confidence through transparent, accountable, and just design, particularly for initiatives like CBDCs.[55] This requires not only technical solutions for security, scalability, and operational efficiency, but also robust public-private partnerships to drive innovation and establish appropriate regulatory frameworks.[56]

V. CONCLUDING REMARKS

The analysis shows that while blockchain offers significant opportunities to enhance transparency, efficiency, and integrity in national financial and administrative systems, its adoption also presents notable legal and governance challenges. The technology's decentralised structure fundamentally changes traditional models of accountability, raising questions about responsibility for system failures, data breaches, and operational errors when no single authority oversees a network. Simultaneously, its immutability and distributed verification mechanisms create tensions with regulatory obligations, especially those related to data correction rights, privacy protection, and system reliability under Indonesian law.

For the national financial system, the most critical implication is how blockchain interacts with Bank Indonesia's mandates as the central bank, particularly its constitutional and statutory authority to regulate payment systems, maintain monetary stability, and ensure the integrity of the rupiah—now including its potential digital form under emerging CBDC frameworks. Similarly, the OJK must anticipate blockchain's impact on market conduct, prudential supervision, and consumer protection.

Therefore, the integration of blockchain into essential financial infrastructure must be developed through a comprehensive, adaptable, and state-focused regulatory framework. This framework should maintain the central bank's independent control over monetary sovereignty, ensure legal clarity, including clear legal accountability for blockchain operators as electronic system providers in the financial system, particularly in cases of electronic system failures or data discrepancies occurring within the blockchain

[55] Ammar Zafar, "Privacy as institutional design: A legal-technological analysis of CBDC governance and compliance". *Computer Law and Security Review*. (April, 2026), 3 https://doi.org/10.1016/j.clsr.2025.106258

[56] Shah, M.A., and Navneet Raj, "Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled CBDC" *Digital Business* Vol. 5 Issue 1, (June, 2025), 2 https://doi.org/10.1016/j.digbus.2025.100111

network, and promote innovation while mitigating systemic risks. Coordinated governance among the central bank, financial regulators, and government bodies will be crucial not only for managing technological vulnerabilities but also for protecting public trust, financial stability, and the long-term viability of blockchain-based services within Indonesia's national financial and monetary system.

REFERENCES

Atzori, Marcella. "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" *Journal of Governance & Regulation* 6, no. 1 (2017): 45–62. https://doi.org/10.22495/jgr_v6_i1_p5.

Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto. *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. IMF Fintech Note No. 2022/007*. International Monetary Fund, September 2022. https://www.imf.org/-/media/files/publications/ftn063/2022/english/ftnea2022007.pdf.

Bank for International Settlements. "*The Next-Generation Monetary and Financial System*." In *BIS Annual Economic Report 2025*. Bank for International Settlements, 2025. https://www.bis.org/publ/arpdf/ar2025e3.pdf.

Basel Committee on Banking Supervision (BCBS). *Prudential Treatment of Cryptoasset Exposures*. Basel: Bank for International Settlements, December 2022. https://www.bis.org/bcbs/publ/d545.pdf.

Bimantara, Gesa, Tri Astuti Handayani, and M. Aqiel Alami. "Legal Analysis of Bitcoin Ownership as a Medium of Exchange in the Digital Financial System." *Hakamain: Journal of Sharia and Law Studies* 4, no. 1 (2021): 64-77. https://doi.org/10.57255/hakamain.v4i1.1358.

Cermeño, Javier Sebastian. Bitcoin and Its Potential Impact on the Financial System. Madrid: BBVA Research, 2016. https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf.

Chhunchha, Yash. "Revolutionizing Financial Institutions: The Influence of Blockchain Technology in the Banking Sector in California." PhD diss., Westcliff University, 2025.

CoinMarketCap. Global Crypto Market Report. 2024. https://coinmarketcap.com.

Guo et al., "Cryptocurrencies and Central Bank Digital Currencies in Global Perspective" *Journal of Risk and Financial Management* Vol. 18 Issue 11, 2025 https://doi.org/10.3390/jrfm18110644

Holloway, Samuel. "Examining the Adoption of Blockchain Technology in Financial Information Systems." *SSRN Electronic Journal,* (2025). https://dx.doi.org/10.2139/ssrn.5121823

Hugo, Alonel. "Private Blockchain-Based Procurement and Asset Management System with QR Code." *SSRN Electronic Journal,* January. (2024) https://doi.org/10.2139/ssrn.4918938

Iansiti, Marco, and Karim R. Lakhani. "The Truth about Blockchain." *Harvard Business Review* 95, no. 1 (2017): 118–127. https://hbr.org/2017/01/the-truth-about-blockchain.

International Monetary Fund. *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risk*. Washington, D.C.: International Monetary Fund, April 2024. https://www.imf.org/en/publications/gfsr/issues/2024/04/16/global-financial-stability-report-april-2024.

International Telecommunication Union. *Digital Financial Services: Regulating for Financial Inclusion–an ICT Perspective*. ITU, 2016.

Khiaonarong, Tanai, and Terry Goh. "Fintech and Payments Regulation: Analytical Framework." IMF Working Paper WP/20/75, International Monetary Fund, Washington, D.C., May 2020.https://www.imf.org//media/files/publications/wp/2020/english/wpiea2020075-print-pdf.pdf

Koonprasert, Tayo Tunyathon, Shiho Kanada, Natsuki Tsuda, and Edona Reshidi, "Central Bank Digital Currency Adoption: Inclusive Strategies for Intermediaries and Users", *Fintech Notes* 2024, No. 005, Washington, DC: International Monetary Fund, 2024, https://doi.org/10.5089/9798400289422.063

Lytvyn, Olena, Volodymyr Kudin, Andrii Onyshchenko, Mykyta Nikolaiev, and Natalia Chaplynska. "Integration of Digital Means in the Financial Sphere: The Potential of Cloud Computing, Blockchain, Big Data and AI." *Financial and Credit Activity: Problems of Theory and Practice* 1, no. 54 (2024): 128–145. 10.55643/fcaptp.1.54.2024.4257.

Mahdani, Rimal, and Dara A. Soufyan. "Blockchain and AI in Combating Financial Corruption: A Systematic Literature Review." *Journal of Central Banking Law and Institutions* 5, no. 1 (2026): 125–152.

Movanu, Luminita. "Blockchain for an Efficient Public Administration". *Perspective Politice 16*, (January, 2023). https://doi.org/10.25019/perspol/23.16.0.13

Nabilou, Hossein. "Bitcoin Governance as a Decentralized Financial Market Infrastructure." *Stanford Journal of Blockchain Law & Policy* 4, no. 2 (2021): 197–240. https://hdl.handle.net/11245.1/baf416c7-5ed7-4b61-8a22-d70d91336bc1.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. https://bitcoin.org/bitcoin.pdf.

OECD. *Competition, Fintechs, and Open Banking: An Overview of Recent Developments in Latin America and the Caribbean*. OECD Roundtables on Competition Policy Papers No. 313. Paris: OECD Publishing, 2024.

Pal, et.al., "Innovation on Credit: The Role of Fintech and Institutional Quality in Global Technological Advancements" *Journal of Innovation and Entrepreneurship* Vol. 14 Issue 1, 2025 https://doi.org/10.1186/s13731-025-00568-8

Pavlov, Roman, Olena Zarutska, Tatyana Pavlova, Tatyana Grynko, Oksana Levkovich, and Liudmyla Hordieieva-Herasymova. "Blockchain as a Management Technology: Institutionalization of Crypto-Assets and Transformation of Entrepreneurial Models Using the Example of Ethereum." *Financial and Credit Activity: Problems of Theory and Practice* 6, no. 59 (2024): 151–66.

Pestovska, Zoriana S. "(R)evoliutsiia bankinhu: Dyskusii ta perspektyvy [(Р)Еволюція Банкінгу: Дискусії та Перспективи," Academy Review *[Пестовська]* 1, no. 54 (2021): 37–47. https://doi.org/10.32342/2074-5354-2021-1-54-4.

Putra, Diky Pratama, and Pujiyono Suwadi, "The Legal and System Security hurdles in Implementing Electronic-Based Government System at the Department Population and Civil Registration in Indonesia." *Advances in Social Sciences, Education and Humanities Research, Proceedings of the International Conference on Cultural Policy and Sustainable Development,* (2024): 612-619.

Republik Indonesia. Law No. 11 of 2008. 2008.

Republik Indonesia. Law No. 21 of 2011 on the Financial Services Authority. 2011.

Republik Indonesia. Law No. 23 of 1999 on Bank Indonesia. 1999.

Republik Indonesia. Law No. 27 of 2022 on Personal Data Protection. 2022.

Republik Indonesia. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. 2019.

Scheltz, et. al. "Blockchain and Regenerative Finance: Charting a Path toward Regeneration." *Frontiers in Blockchain,* (July, 2023), 7 https://doi.org/10.3389/fbloc.2023.1165133

Shah, M.A., and Navneet Raj, "Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled CBDC" *Digital Business* Vol. 5 Issue 1, (June, 2025). https://doi.org/10.1016/j.digbus.2025.100111

Shoetan, Philip Olaseni, and Babajide Tolulope Familoni. "Blockchain's Impact on Financial Security and Efficiency." International Journal of Management & Entrepreneurship Research 6, no. 4 (2024): 1213.

Swan, Melanie. *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

Tan, Evrim, Stanislav Mahula, and Joep Crompvoets. "Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management." *Government Information Quarterly* 39, no. 1 (2022): 101625. https://doi.org/10.1016/j.giq.2021.101625.

Tsouris, Ioannis, Georgios L. Thanasas, Maria Rigou, "Assessing the European Central Bank's Institutional Capacity Readiness for the Introduction of the Digital Euro" *Journal of Risk and Financial Management* Vol. 19 Issue 2, (February, 2026), https://doi.org/10.3390/jrfm19020148

Udeh, Ezekiel Onyekachukwu, et al. "The Role of Blockchain Technology in Enhancing Transparency." Finance & Accounting Research Journal 6, no. 6 (2024): 836.

Zafar, Ammar. "Privacy as institutional design: A legal-technological analysis of CBDC governance and compliance", *Computer Law and Security Review.* (April, 2026). https://doi.org/10.1016/j.clsr.2025.106258

Zhang, Tao, and Zhigang Huang. "Blockchain and Central Bank Digital Currency." *ICT Express* 8, no. 2 (2022): 264-70. https://doi.org/10.1016/j.icte.2021.09.014.