Int. j. adv. multidisc. res. stud. 2026; 6(6):1080-1090

Received: 06-10-2026
Accepted: 16-11-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Legal Challenges in the Implementation of Blockchain Technology and Smart Contracts for Securities Transaction Settlement on the Stock Exchange

[1] Iswi Hariyani, [2] Edi Wahjuni, [3] Moh Ali, [4] Gatot Iriyanto, [5] Bhim Prakoso
[1, 2, 3, 5] University of Jember, Indonesia
[4] Moch Sroedji University, Indonesia

Corresponding Author: **Iswi Hariyani**

Abstract
The development of blockchain technology and smart contracts offers high efficiency through instant settlement of securities transactions. However, the Indonesian capital market still relies on a centralized clearing mechanism (T+2). This study aims to analyze the legal validity of smart contracts in securities transactions, the legal implications of blockchain's decentralization on the existence of centralized institutions (KPEI and KSEI), and the legal liability in the event of an electronic system failure. The research method applied is normative legal research with statutory and conceptual approaches. The results indicate that although smart contracts are formally valid as electronic contracts under the Indonesian Civil Code and the ITE Law, their full implementation clashes with the Capital Market Law which mandates centralized clearing institutions. Furthermore, there is a legal vacuum regarding risk mitigation and civil liability in the event of a system glitch or programming code failure. In conclusion, the current Indonesian positive law is not fully prepared to accommodate this technology entirely. This study suggests that the Financial Services Authority (OJK) optimize the Regulatory Sandbox and harmonize regulations within the Capital Market Law to provide legal certainty for future capital market innovations.

Keywords: Capital Market, Blockchain, Smart Contract, Securities Transaction

1. Introduction

1.1 Background

The capital market plays a crucial role as a key pillar driving the national economy and serves as a financing vehicle for the business sector in the digital economy era.[1] Amidst the massive wave of globalization and the quantum leap in financial technology, market demands for faster, more secure, efficient, and transparent securities transaction processing have become an unavoidable, fundamental necessity.[2] However, under the current conventional capital market architecture, the securities transaction settlement process still relies on a centralized mechanism with a T+2 timeframe (two business days after the transaction is agreed upon on the exchange).

Reliance on this centralized clearing model is considered to trigger significant counterparty risk and create liquidity imbalances due to settlement lags. In an era of rapid global financial technology advancement, this conventional settlement model is often viewed as insufficiently responsive to high market volatility and is deemed to reduce capital efficiency for both retail and institutional market participants.[3] Therefore, modernizing the clearing architecture through decentralized innovation or real-

[1] K.S. Aulia, Sitorus, M., & Batubara, M. Peran Pasar Modal dalam Perekonomian Indonesia. JIKEM: Jurnal Ilmu Komputer, Ekonomi Dan Manajemen, 2(2), (2022). 2523–2529.
[2] K.A. Maspul, & Putri, A. Teori digitalisasi pasar modal: Pengaruh digitalisasi terhadap efisiensi pasar keuangan. *Journal of Innovative and Creativity*, 1(1), (2025). 12-25.
[3] Sella, S., dkk. Transformasi manajemen pasar modal di era digital. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 5(2), (2026). 112-125.

time settlement systems has become a crucial imperative to minimize cyber risks and ensure full transparency.[4] This bureaucratic chain involves numerous banking intermediaries and state-appointed central custodians. Although the system is considered well-established, the presence of these third-party intermediaries inherently entails high transaction costs, the risk of failure to deliver investment products, and vulnerability to centralized data system failures.[5] The inherent flaw of this model lies in the high accumulation of intermediary fees and the existence of a settlement lag, which heightens the risk of failure to deliver securities or funds. Furthermore, total reliance on a single infrastructure creates the risk of systemic paralysis in the event of a single point of failure or an electronic system breakdown affecting the centralized data.

In the modern capital market ecosystem, reliance on a single clearing entity is considered to constrain market liquidity due to settlement time lags. When an investor executes an order, the legal transfer of asset ownership is not fully recognized until the inter-institutional reconciliation process is completed 48 hours later. This structural delay ties up capital—incurring associated costs—and heightens counterparty credit risk, particularly during periods of extreme market volatility. Amidst the rigidity of traditional capital market systems, the innovation of distributed ledger technology (DLT)—commonly known as blockchain technology—emerged and was integrated with smart contract systems. This innovation sparked a global wave of financial asset tokenization, wherein conventional securities such as stocks, bonds, and mutual funds are converted into encrypted digital representations on distributed networks.[6] This technology offers a new disruptive paradigm of radical decentralization, wherein every transaction record is permanent, transparent, and capable of instant settlement without the need for manual confirmation or validation by a central clearinghouse.

The term "smart contract" refers to an autonomous computer protocol capable of automatically executing agreements based on lines of computer code once the objective conditions agreed upon by the parties have been met. Globally, empirical research indicates that transitioning clearing infrastructure to real-time settlement systems can reduce inter-party coordination costs and generate massive annual opportunity cost efficiencies within the global financial sector.[7] When conventional intermediaries are substantially eliminated, market liquidity increases exponentially because the transfer of funds and securities occurs simultaneously within seconds. Global giants such as BlackRock, BNY Mellon, and JPMorgan Chase—through the Kinexys platform—have tangibly demonstrated this operational advantage in managing digitized assets.[8] Despite offering a revolutionary leap in efficiency, the discourse and urgency surrounding the implementation of blockchain technology and smart contracts within the securities transaction mechanisms of the Indonesia Stock Exchange (IDX) clash directly with aspects of national positive law. Indonesia adheres to a civil law system where regulations rely heavily on rigid, written statutory texts, whereas this technology operates based on the logic of autonomous digital code that transcends national jurisdictional boundaries.

The wide gap between the rapid pace of technological innovation and the rigidity of legal regulations gives rise to multidimensional legal uncertainty challenges spanning three fundamental domains, namely:

First, from the perspective of contract law, smart contracts employ a computer programming code scheme that automatically replaces the role of human legal language. This characteristic of absolute automation—devoid of human legal subject intervention—raises fundamental issues regarding legal validity within national civil law. The Indonesian civil law regime strictly delineates the parameters for contract validity under Article 1320 of the Civil Code, which requires free consent, the parties' legal capacity to act, a specific subject matter, and a lawful cause. When a securities transaction agreement is negotiated via a user interface, algorithmically locked, and automatically executed by a consensus-based computer network, the boundaries of "free agreement" become highly ambiguous and difficult to substantiate within the framework of traditional civil law.[9] The operational structure of smart contracts, adhering to the "code is law" principle, means that once the code is uploaded to the blockchain network, it executes autonomously and deterministically; it cannot be unilaterally revoked, altered, or suspended, even in the event of a discrepancy in the parties' intentions.

Theoretically, within international digital contract law, a significant debate has emerged regarding the "reasonable coder" interpretation concept used to determine the parties' intentions in instances of computer code logic errors or discrepancies between written legal text and its code representation.[10] Although Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) has legitimized electronic contracts, existing regulations do not specifically address the characteristics of contracts in the form of self-executing code—which require neither intermediary agents nor human intervention to execute performance. Consequently, examining the alignment of the autonomous nature of smart contracts with

[4] R. M. Mukhlasin, & S. A. P. Rahayu, Transformasi hukum pasar modal di era digital: Pilar Investasi Dan Pembangunan Ekonomi. *YUSTISI*, 12(3), (2025). 45-58.

[5] E. Siswanto, dkk. Reformasi Financial Flow melalui Tokenisasi Real World Asset (RWA): Analisis Desentralisasi dan Interoperabilitas Keuangan Global. *Kajian Jurnal Manajemen dan Bisnis (KJMB)*, 3(2), (2025). 85-98.

[6] Deloitte Insights. *Banking and Capital Markets Outlook: The Structural Shifts in Digital Asset Infrastructures*. Financial Services Review (2025).

[7] Babar, A., & Wu, X. *FinTech Transformations: Decentralized Automation and Technical Risks in Financial Sectors*. Journal of Green FinTech and Financial Innovation, 14(1), (2025). 8-22.

[8] National Law Review. *How Wall Street's Trillion-Dollar Crypto Infrastructure Push is Redefining Portfolio Diversification and Clearing Rail Systems*. NLR Journal, (2026).

[9] Fakhriah, S., Hans, S. W. P., & Syamsul. *Analisis Yuridis Keabsahan Smart Contract Dalam Perspektif Hukum Perdata Indonesia*. Jurnal Kepastian Hukum dan Keadilan, 7(1), (2025). 40-55.

[10] Szabo, J., Bernard, C., & Philip, L. *Implications and Challenges of Blockchain Technology and Smart Contracts*. Computer Life Journal (University of Kansas & University of Iowa School of Law), 12(2), (2024). 6-25.

national principles of contract law has become a pressing legal issue that must be addressed to ascertain their legal status.

Secondly, from the perspective of capital market law and institutional frameworks, the defining characteristic of blockchain technology—decentralization—stands in diametric opposition to the regulatory foundation of Law Number 8 of 1995 concerning Capital Markets (the Capital Market Law). The legal architecture of Indonesia's capital market is built upon a doctrine of protective centralization. The law is imperative and centralistic in nature, explicitly mandating that the activities of clearing, guaranteeing, and settling securities transactions must be conducted by authorized state-sanctioned monopolies: the Clearing and Guarantee Institution (LKP) and the Depository and Settlement Institution (LPP). In the context of the Indonesian capital market, these crucial functions are performed by PT Kliring Penjaminan Efek Indonesia (KPEI) and PT Kustodian Sentral Efek Indonesia (KSEI).

If stock exchanges transition to blockchain technology, the processes of validation, ownership recording, and securities transaction settlement would be entirely taken over by a distributed computer network (nodes or validators) utilizing cryptographic consensus mechanisms. This architectural shift would automatically negate and obscure the legal status, core duties, functions, and self-regulatory authority vested in KPEI and KSEI under Capital Market Law provisions. Internationally, global regulatory bodies such as IOSCO have emphasized the importance of "technology-neutral regulation," whereby digitally defined securities must still adhere to issuer protection standards and legal obligations equivalent to those of conventional securities, even when settlement is executed through smart contract automation.

Furthermore, global initiatives such as Project Agora by the Bank for International Settlements (BIS) demonstrate how the integration of digital assets requires a robust interconnection between private international law and shared ledger technology.[11] In various other developing countries, capital market regulations are also undergoing major overhauls to provide jurisdictional certainty specifically for these autonomous digital contracts.[12] In Indonesia, the lack of clarity regarding the operational boundaries of this decentralized technology within capital market laws creates a risk of institutional overlap. The absence of regulatory guidelines concerning the relationship between decentralization and the authority of central institutions could trigger a systemic legal vacuum if implementation is forced without first restructuring the legal framework governing capital market institutions.

Third, regarding risk mitigation and legal liability, technology is empirically never free from error. Although blockchain networks are touted for their high security due to cryptographic encryption, the code underlying smart contracts remains potentially vulnerable to system malfunctions, cyberattacks, hardware failures, and flaws in programming logic. Recent security reports indicate that financial losses resulting from smart contract vulnerabilities have surged dramatically, reaching tens of millions of dollars at the institutional level.[13] A United States court ruling in the case of *United States v. Spalletta* affirmed that exploiting vulnerabilities in smart contract code can be classified as a criminal offense involving computer misuse, indicating that the judicial system is being compelled to respond to the functional failures of this technology.

In conventional stock exchange transaction mechanisms, should an electronic trading system failure occur, KPEI legally acts as the ultimate guarantor, bearing the legal responsibility to resolve disputes and safeguard the rights of securities holders through the guarantee fund it manages. Conversely, in a blockchain ecosystem—characterized by the absence of intermediaries and the principle of data immutability—there are significant risks, such as "oracle risk" (errors in supplying external real-world data to the digital system) and ambiguity regarding civil liability attribution should investor capital be lost due to algorithmic code failure.[14] Due to the nature of blockchain without intermediaries, when a system malfunction occurs, it is legally unclear who bears the status as defendant—whether the creator of the program code (developer), the network validators, or the stock exchange platform that facilitates it.

Moreover, the permanent transparency of blockchain also risks conflicting with the right to privacy and the right to delete retail investors' data in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Any financial transaction data recorded on the blockchain cannot be deleted, even though the PDP Law guarantees the data subject's right to delete their personal data. This data privacy legal dilemma has also become a fierce debate in aligning this technology with the General Data Protection Regulation (GDPR) instrument in the European Union.[15] The absence of regulations regarding the legally liable parties and civil compensation mechanisms for the failure of this autonomous technology creates massive legal uncertainty for public investors and capital market consumers.

Based on the foregoing, there is a clear gap between the accelerating digitalization of global financial markets and the state of legal regulation in Indonesia. If this legal challenge remains unaddressed by comprehensive academic and regulatory solutions, Indonesia risks not only missing opportunities to enhance its global capital market competitiveness but also plunging the national investment climate into legal uncertainty that threatens financial stability. Driven by this empirical and theoretical urgency, this legal research focuses on assessing the readiness of civil law regulations, unraveling institutional overlaps within the capital market, and formulating an ideal regulatory framework and legal liability model for the utilization of

[11] Bruegel Policy Brief. *A new strategy to contain stablecoin risks in the European Union*. Brussels Financial Studies Series, (2026).

[12] PwC Global Crypto Regulation Report. *Regulatory Developments in Selected Jurisdictions for Capital Market Innovations*. PwC Financial Services Network (2026).

[13] Hacken Security Report. *Q1 2026 Security & Compliance Report: Smart Contract Vulnerability Losses and Institutional Protocols Risk Mitigation*. Hacken Compliance Docs. (2026).

[14] Nishith Desai Associates. *Vulnerabilities in Smart Contracts and Cybersecurity Laws for Controllable Electronic Assets*. Technical Law Review, Polymath Network Research Series (2025).

[15] Oxford Academic Cybersecurity. *Reconciling Blockchain Technology and Data Protection Laws: Evolving Interpretations of Immutability and Joint Controllership*. Cybersecurity Law Journal, 11(1), (2025), h.2.

blockchain technology and smart contracts on the Indonesia Stock Exchange. Consequently, three issues will be examined in depth:

1. What is the legal validity of using smart contracts in securities transactions within the capital market, viewed from the perspective of Indonesian contract law and the Law on Electronic Information and Transactions?
2. What are the legal implications of applying the blockchain technology decentralization principle for the existence of KPEI and KSEI under the Capital Market Law?
3. What forms of risk mitigation and legal liability apply in the event of an electronic system failure resulting from a cyberattack on blockchain-based securities transactions?

2. Discussion

2.1 The Juridical Validity of the Use of Smart Contracts in Securities Transactions in the Capital Market Viewed from Indonesian Contract Law and the Electronic Information and Transactions Law

Technically, a smart contract is a sequence of autonomous code stored and executed on a blockchain network based on "if-then" algorithmic logic. The technology's key characteristic lies in its ability to eliminate the role of third parties (deintermediation), as the rights and obligations of the parties involved are automatically executed by a computer system without the need for human intervention or intermediary institutions. [16] From the perspective of Indonesian positive law, smart contracts are considered legally valid as an extension of "Electronic Contracts," as regulated under the ITE Law and Government Regulation 71/2019. However, the implementation of this technology within the capital market's securities transaction ecosystem gives rise to a duality regarding legal certainty and sharp doctrinal conflicts concerning the following aspects:

1. Fulfillment of Requirements for the Validity of the Agreement

a) Deconstruction of Conventional Civil Law Principles

The self-executing and immutable nature of smart contracts inherently eliminates any scope for the parties to renegotiate. This code-based rigidity challenges the doctrine of good faith and the traditional principle of consensualism, particularly in the event of market anomalies or *force majeure* situations that require human discretion.[17]

b) Challenges Regarding Legal Capacity

Within blockchain-based stock exchange infrastructure, systems execute transactions using pseudonymous addresses or full anonymity, bypassing real-time physical identity verification. This characteristic inherently creates a legal loophole that risks conflicting with the subjective requirements for the validity of agreements—as stipulated in Article 1320 of the Indonesian Civil Code and Article 46 paragraph (2) of Government Regulation No. 71/2019—particularly regarding the legal capacity of economic actors to act as parties to a formal contract.

c) Dualism in Sectoral Regulation

Although the enactment of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (UU P2SK) has reinforced the legal recognition of financial sector technological innovations (ITSK), this legislation lacks adequate implementing regulations—creating a regulatory gap. To date, there remains a void in technical regulations bridging the gap between digital evidentiary law and the limits of strict liability. This uncertainty becomes critical in the event of technical failures (bugs) in smart contract code or system paralysis caused by cyberattacks on stock exchanges. Without clearly defined liability boundaries among system operators, code developers, and exchange authorities, the recovery of investor losses—and thus investor protection—becomes difficult to execute, potentially undermining the credibility of the national capital market.

2. Legitimacy under the ITE Law and P2SK Law Regimes

Within the structure of Indonesian positive law, the existence and legal legitimacy of smart contracts receive strong legal recognition through the attribution scheme set forth in Article 1, point 17 of Law Number 11 of 2008 concerning Electronic Information and Transactions—as amended several times, most recently by Law Number 1 of 2024 (the ITE Law). This provision explicitly classifies these digital instruments as agreements accommodated within an electronic system.[18] As an autonomous code-based mechanism, a smart contract is legally binding on the parties involved—by virtue of the mandate under Article 18 paragraph (1) of the ITE Law—provided that its technical characteristics meet the standards for cyber system reliability.

This standardization is governed by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), which mandates that algorithmic code sequences be secure, reliable, and capable of minimizing the risk of systemic failure. Provided these conditions are met, the algorithmic code transforms into binding law—in accordance with the principle of *pacta sunt servanda* within Indonesia's cyberspace—namely:

a) Within the architecture of future decentralized stock exchanges, the use of private keys by investors to validate and authorize each transaction on the blockchain network normatively meets the legal qualifications of an Electronic Signature (TTE). This asymmetric cryptography validation mechanism is legally valid as it aligns with the provisions of Article 11 paragraph (1) of the ITE Law.[19] This technology ensures that the data used to generate the Electronic Signature (TTE) is exclusively linked to its owner and

[16] A. R. Pratama, Menguji Asas Kebebasan Berkontrak Dalam Smart Contract. *Journal of Electronic Research and Legal Innovation (JERKIN)*, 4(1), (2026). 32-45.

[17] R. Harahap, dkk. *Tantangan Anonimitas dan Peran Identitas Digital dalam Implementasi Smart Contract Berbasis Blockchain*. Jurnal Lex Patri, 14(2), (2026). 1155-1170.

[18] R. L. O., Sitorus dkk. Analisis Yuridis Keabsahan Smart Contract Sebagai Bentuk Perjanjian Elektronik di Indonesia. *Jurnal Ilmiah Penelitian Mahasiswa (JIPM)*, 3(6), (2025). 394–406.

[19] Darwis, M., & Hidayat, R. Keabsahan Dan Kekuatan Pembuktian Tanda Tangan Elektronik Pada Transaksi Bisnis Modern. *Jurnal Mahkamah Hukum Islam (MHI)*, 4(1), (2026). 72–88.

remains under the signer's full control during the authentication process. The complex mathematical configuration within this stock exchange network inherently establishes the characteristic of non-repudiationl.[20] Consequently, any securities transaction signed with a private key cannot be manipulated or unilaterally repudiated by the investor; furthermore, the records within the distributed ledger serve as civil legal evidence possessing valid and binding evidentiary weight.

b) Within the Indonesian civil procedural law framework, the status of digital evidence has been significantly strengthened and accorded solid legal certainty through the provisions of Article 44 paragraph (2) of the P2SK Law. This provision explicitly affirms that smart contracts—along with all their print-outs—are recognized as valid legal evidence in court proceedings, provided that their mechanisms meet the reliability standards for Electronic Contracts as stipulated in the cyber law framework of the ITE Law.[21] Consequently, the entire digital footprint and financial transaction data records distributed across the blockchain network are legally recognized as valid Electronic Information and/or Electronic Documents with binding legal force. Integrating these operational norms not only expands the scope of conventional evidence under Article 1866 of the Civil Code and Article 164 of the HIR but also mitigates the risk of digital evidence being rejected in court due to the absence of a physical form. As a result, the validity of the distributed ledger within the capital market ecosystem transforms into that of a digital authentic document possessing conclusive evidentiary weight, binding force, and full enforceability by law enforcement authorities. Smart contracts are formally valid and recognized as electronic contracts under the legal framework of the ITE Law, the P2SK Law, and the Civil Code. However, in terms of substance within the capital market sector, their validity is legally flawed if designed in a fully decentralized manner without the involvement of KPEI and KSEI. To ensure smart contracts possess legally valid executory power, the technical programming code must be legally modified to designate the official central clearing and depository institutions as the holders of final validation authority.

2.2 Legal Implications of Implementing the Decentralization Principle of Blockchain Technology on the Existence of KPEI and KSEI According to the Capital Market Law

Blockchain technology is disrupting the Indonesian capital market by eliminating the roles of clearing houses and central custodians. Through a distributed ledger system, transaction validation and the recording of asset ownership are performed collectively by a computer network using consensus algorithms. This architectural shift radically challenges the function of centralized intermediary authorities—roles traditionally defined by statute. This automated consensus model eliminates the risk of a total system outage (single point of failure) and accelerates transaction settlement to real-time (T+0). Consequently, blockchain represents not merely a technological upgrade for the exchange, but a fundamental shift in legal paradigms that completely overhauls the concept of liability for clearing houses and central custodians.

This architectural structure stands in diametrical opposition to the Indonesian capital market legal framework, which is founded on a doctrine of protective centralization mandatorily prescribed by the Capital Market Law. Contemporary analysis of economic civil law indicates that a reform of legal norms is imperative to enable colonial and conventional laws to adapt to the dynamics of digital market efficiency.[22] The clash between decentralized blockchain systems and centralized regulation has sparked legal uncertainty in the Indonesian capital market. This conflict arises because the borderless and permissionless nature of blockchain stands in stark contrast to national laws that are rigid, territorially bound, and reliant on authorization from supervisory authorities. The Capital Market Law mandates that securities clearing and depository activities be monopolized by state-designated institutions such as KPEI and KSEI. When these functions are replaced by blockchain algorithms, a legal vacuum arises regarding liability in the event of a system failure. This uncertainty hinders technology adoption, triggers risks of jurisdictional disputes, and threatens investor protection:

1. Implications for Securities Clearing and Guarantee Functions

Pursuant to Article 1 point 6 in conjunction with Article 25 of the Capital Market Law, the activities of clearing and guaranteeing the settlement of securities transactions must be conducted on a monopoly basis by a Clearing and Guarantee Institution (LKP) that has obtained an official business license from the Financial Services Authority (OJK); in this instance, these activities are carried out solely by KPEI. In this capacity, KPEI legally acts as the Central Counterparty. Based on civil law doctrine, KPEI engages in a legal relationship known as civil novation, whereby it terminates the direct contractual relationship between the seller and buyer of the underlying securities on the exchange and interposes itself as the buyer to the seller and the seller to the buyer. Normatively, this measure aims to guarantee the fulfillment of the parties' rights and obligations—in the event that one party experiences a failure to deliver or a failure to pay—in order to maintain market stability.

If stock exchange architecture shifts to blockchain technology, transaction settlement processes can transition to an atomic settlement scheme—or real-time simultaneous delivery-versus-payment. Through the integration of smart contracts, the transfer of tokenized securities ownership and funds between investors occurs simultaneously within seconds at the network level, eliminating the need for the conventional T+2 clearing lag. From a technological standpoint, this instant settlement capability effectively

[20] Ramli, A. F. Implikasi Perkembangan Teknologi Blockchain Terhadap Hukum Pembuktian Perdata di Indonesia. *Jurnal Urusan Riset dan Inovasi Hukum (JURRISH)*, 2(1) (2026), 44–59.

[21] Monika Esterina Situmorang, Analisis Aspek Hukum Kontrak Pintar dalam Transaksi Kebendaan Digital: Tantangan Anonimitas dan Peran Identitas Digital, *Lex Patrimonium*, Vol. 4, Iss. 1 [2025], 1-25.

[22] Sugiswati, *et al*. *A Review of Civil Law Literature on Sales Contracts, Money Lending Agreements, and Smart Contract Integration for Indonesia Emas 2045*. International Journal of Economic and Financial Issues, 6(2), (2026). 1040-1046.

removes the need for mechanisms to guarantee against counterparty default risk, as the smart contract will not execute the transaction if either party lacks sufficient securities or funds in their digital wallet. Technical framework proposals from global capital market regulators even project cost efficiencies amounting to billions of dollars through the automation of post-trade processing driven by smart contracts.

From a legal standpoint, the elimination of the need for guarantees obscures the essence of the mandate set forth in Articles 25 and 26 of the Capital Market Law, which require the existence of clearing regulations and the management of a centralized guarantee fund. If a blockchain system operates purely without the involvement of a central clearing agency, such transactions are classified as a violation of capital market laws because clearing is conducted outside the official monopoly entity designated by statute. KPEI risks losing its civil legal operational basis if contract novation is no longer required within a self-executing system.

2. Implications for Central Depository and Settlement Functions

The second institutional aspect directly affected is the Depository and Settlement Institution (LPP), which is officially operated by KSEI pursuant to Article 1 point 7 in conjunction with Article 27 of the Capital Market Law. KSEI plays a central role in providing central depository services, centralized securities account recording, and the settlement of securities transactions via book-entry transfer. Capital market regulations stipulate that records in securities accounts at KSEI constitute valid proof of securities ownership for investors. Blockchain technology inherently functions as a ledger for recording asset ownership—distributed transparently and permanently across network nodes—that does not rely on a single, centralized database. An investor's ownership rights to a digital share are directly tied to the possession of a private key that is validly recorded on the blockchain.

This paradigm of decentralized securities ownership recording creates a fundamental overlap of legal functions. If ownership records on the blockchain are deemed legally valid and binding, then the monopoly authority held by KSEI—as the central administrator of securities—over the recording process becomes functionally irrelevant. Conversely, if positive law insists on recognizing only KSEI's internal computer records as the sole legally valid proof of securities ownership, then the use of blockchain will merely become a redundant technological layer—creating extra work without delivering operational efficiency. Investors would be forced to wait for manual synchronization between blockchain data and KSEI's database, thereby undermining the very essence of speed offered by distributed ledger technology.

3. Institutional Reconstruction Solution: The Permissioned Blockchain Concept and the Role of the Central Institution as a Super-User

To bridge the gap between the principle of technological decentralization and Indonesian public law governing capital markets, blockchain adoption cannot proceed without constraints. The Indonesia Stock Exchange is required to implement a permissioned, limited distributed network model. Under this governance framework, the legal functions and status of KPEI and KSEI are not eliminated but rather functionally reconstructed in accordance with the principle of technology neutrality recommended by the global regulatory body IOSCO.

The IOSCO report strongly emphasizes that tokenized securities must adhere to the same rigorous standards as conventional securities regarding issuer disclosure, settlement finality, and the responsibilities of underwriters. This alignment in governance also mirrors global asset digitalization roadmaps—such as the Bank for International Settlements' (BIS) Project Agora—which integrate traditional finance (TradFi) with decentralized infrastructure using the ISO 20022 global interoperability communication standard.[23] The technical and legal implementation of this role reconstruction can be broken down into three operational pillars:

a) KPEI and KSEI as Multi-Signature Validator Nodes

The central clearing institution is positioned as the key authority and primary validator within the capital market network. A securities transaction is deemed legally valid and included in a new block only after receiving digital validation from KPEI and KSEI through a specialized consensus mechanism. In this manner, the centralization of clearing functions mandated by the Capital Market Law continues to satisfy regulatory requirements while aligning with the OJK's policy priorities regarding digital financial assets.[24]

b) KSEI as the Supervisor of Identity Management and the Custodian Gateway

KSEI holds the legal role of sole administrator responsible for matching an investor's authentic real-world digital identity (Know Your Customer) with their digital wallet address on the blockchain network. This is crucial for ensuring full compliance with the Personal Data Protection (PDP) Law, under which KSEI acts as the Personal Data Controller, shielding retail investors' data privacy from public view.

c) KPEI as the Administrator of Emergency Rollback and the Digital Guarantee Fund

KPEI no longer handles daily clearing manually; instead, it acts as a market oversight body with the authority to exercise emergency overrides. In the event of a programming code failure, KPEI is empowered by special rights within the smart contract to temporarily freeze transactions or execute a limited rollback to safeguard the stability of the national financial system.

The pure application of the blockchain decentralization principle implies the loss of the necessity for centralized institutions such as KPEI and KSEI, which in turn contravenes the mandatory provisions of the Capital Market Law. To ensure the legality of this innovation, Indonesian capital market law must redefine "clearing and depository institutions"—shifting the definition away from entities

[23] International Organization of Securities Commissions (IOSCO). (2025). *Regulatory Models, Investor Protection, and Responsible Adoption in Digital Capital Markets*. IOSCO Public Reports, ResearchGate Brief.

[24] Financial Services Authority of Indonesia (OJK). *Deepening Digital Financial Assets and Crypto Ecosystem Ecosystems*. Press Release of OJK Annual Financial Industry Industry Meeting, Jan 2026.

serving as physical repositories and centralized single databases, and toward entities that hold the authority to validate the governance of distributed ledger systems. Future OJK regulations need to be geared towards facilitating the restructuring of this institutional role to align with the era of global financial asset digitalization.

2.3 Forms of Risk Mitigation and Legal Liability in the Event of Electronic System Failure Resulting from Cyberattacks on Blockchain-Based Securities Transactions

The implementation of blockchain technology and smart contracts within stock exchange infrastructure does not automatically create a capital market ecosystem that is entirely immune to the risk of functional failure. Although these decentralized systems offer advantages such as data resilience and minimized human intervention, their architecture remains vulnerable to programming logic flaws and technical malfunctions within the embedded algorithmic code. When rigid and immutable smart contracts automatically execute flawed code, the system lacks the discretionary capacity to halt transactions instantly, potentially triggering massive financial losses for investors.[25] Furthermore, reliance on external oracles to supply real-time price data to the blockchain network introduces new vulnerabilities, specifically oracle manipulation attacks and structured cyber intrusions.[26]

Consequently, this potential for operational paralysis not only results in large-scale material losses but also triggers legal uncertainty regarding the limits of civil liability and the allocation of the burden of digital proof among the disputing parties. Despite the robust cryptographic defenses afforded by decentralized consensus mechanisms, distributed ledger technology ecosystems remain susceptible to latent vulnerabilities involving various forms of technical disruption and structured cyberattacks. At the physical infrastructure level, these systems are still vulnerable to hardware failures at network nodes, code malfunctions resulting from human error, and the risk of external data manipulation—specifically "oracle risk"—which threatens the accuracy of real-time price data feeds.

Furthermore, this autonomous nature is not entirely immune to advanced security exploits at the protocol layer. These digital threat vectors range from 51% attacks—which compromise consensus integrity by seizing a majority of computing power—and Sybil attacks—which fabricate numerous identities to dominate network voting authority—to reentrancy exploits that leverage programming logic flaws in smart contract protocols to illicitly drain digital assets.[27] Consequently, the complexity of these multidimensional threats underscores that blockchain reliability cannot be taken for granted; instead, it requires layered cybersecurity audits and dynamic, risk-mitigating regulatory frameworks to ensure investor protection and the operational stability of exchanges.

In the Indonesian conventional capital market architecture, the risk of trading system failure has been rigidly anticipated by the Clearing and Guarantee Institution (LKP) which acts as the Central Counterparty (CCP) to guarantee transaction settlement by law. Based on the juridical mandate of Article 14 of the Capital Markets Law, KPEI as LKP mitigates the risk of failure to hand over securities or funds through a mechanism for guaranteeing the settlement of stock exchange transactions via the principle of legal innovation as well as managing guarantee funds.[28] Conversely, the self-executing and immutable nature of blockchain introduces new complexities regarding the attribution of civil liability and the determination of the legal entity liable for damages.[29]

Namely, the collapse of the doctrine of liability based on fault—as stipulated in Article 1365 of the Indonesian Civil Code—resulting from the absence of a single, centralized intermediary.[30] In the event of a functional failure, the determination of the legal subject becomes ambiguous due to the dispersed nature of the exchange's operational control. A study of digital civil law maps out the proportional allocation of legal liability among code developers—based on professional negligence—the stock exchange authority as the primary platform provider, and the parties executing the consensus, namely:

1. Allocation of Civil Legal Liability

In the event of an electronic system failure or cyberattack resulting in the loss of digital securities assets or a mass failure of transaction settlement, the determination of legal liability must be examined through the lens of civil law instruments and national information technology regulations. This entails combining the doctrine of Unlawful Acts (Article 1365 of the Indonesian Civil Code) with the strict liability regime applicable to Electronic System Providers (PSE), as mandated by Article 15 of the ITE Law and Article 46 of Government Regulation (PP) on Electronic System and Transaction Providers (PSTE).

Under this regulatory framework, the stock exchange, acting as an Electronic System Provider (PSE), bears joint and several legal liability for any losses incurred, unless it can prove that the failure was caused solely by *force majeure* or the user's own fault..[31] However, given the disintermediated nature of blockchain and smart contract architectures, national civil law frameworks face the challenge of expanding conventional concepts of civil legal

[25] Fransisco, W. (2026). Blockchain-based smart contracts: Legal certainty and regulatory implications within the Indonesian contract law framework. *Jurnal Hukum dan Keadilan*, 5(1), 12–30.

[26] Kurdi dkk, Legal Analysis of Smart Contracts as Electronic Agreements under Civil and Electronic Transactions Law, *Jurnal Hukum Magnum Opus*, olume 9 Nomor 1 (2026): 56-67.

[27] Arry Maulana Syarif dkk, *Blockchain: Konsep Dan Arsitektur*, (Semarang, Ritecs, 2026), h.151.

[28] Yofi Satriya Wijaya, Tinjauan Yuridis Peran PT Kliring Penjaminan Efek Indonesia Sebagai Central Counter Party Untuk Transaksi Derivatif Suku Bunga Dan Nilai Tukar Over the Counter, *Jurnal Dharmasisya*, Vol 1 No 3 (2021) 1603-1614.

[29] Dimas Winky Siantu Setyo Negoro dkk, Keabsahan Smart Contract Berbasis Blockchain Menurut Hukum Transaksi Perdagangan Indonesia, *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 6(1), (2026), 105–119.

[30] Hapsari, A. W., & Laia, A. Kedudukan Hukum Smart Contract Dalam Sistem Perjanjian Menurut Hukum Perdata Indonesia. *Jejak Digital: Indo Jurnal Press*, 2(4), (2026). 8611-8621.

[31] Ana Tasia Pase, Perlindungan dan Kepastian Hukum Terhadap Transaksi *e-Contract* dalam Perjanjian Digital di Indonesia, *Yustitiabelen*, Vol. 12 No. 2 (2026), h.1-29.

subjects to encompass software developers—on grounds of professional negligence—as well as the network validators who collectively execute consensus[32], namely:

a) Legal Liability of Electronic System Providers (PSE):
The stock exchange, KPEI, and KSEI—which operate permissioned blockchain networks within the capital market—are classified as Electronic System Providers (PSE). Pursuant to Article 15 of the ITE Law, a PSE is required to ensure the reliability and security of its electronic system and to operate said system in a reliable, secure, and responsible manner. Should investor losses arise from negligence in system governance, inadequate encryption oversight, or the failure to address foreseeable security vulnerabilities (gross negligence), the governing institution may be sued for an Unlawful Act (PMH) under Article 1365 of the Indonesian Civil Code, thereby becoming liable for the full extent of the investors' material damages.

b) Limitation of Liability Clause and the Doctrine of Digital Force Majeure
If the failure is caused by an external hacker exploiting a previously undetected vulnerability in new programming code, the limits of legal liability hinge on the enforceability of exclusion clauses within the initial electronic contract. Modern economic civil law jurisprudence and doctrine have begun to classify massive-scale cyberattacks or global consensus malfunctions as forms of "Digital *Force Majeure*" [United States v. Spalletta]. This digital *force majeure* exempts the Electronic System Provider (PSE) from civil liability for damages, provided the PSE can demonstrate full compliance with code audit standards (smart contract audit verification), the implementation of international cybersecurity standards (ISO/IEC 27001), and the execution of appropriate technological due diligence.

c) Civil Liability of the Developer/Coder
Based on the "code is law" principle of autonomization, the execution of computer code is regarded as a reflection of the parties' contractual agreement. Architects or programmers cannot be held personally civilly liable for systemic exchange failures. However, a clear legal exception applies if elements of bad faith are established—specifically, the inclusion of hidden code intentionally embedded to facilitate asset theft or securities price manipulation. In such instances, liability shifts from civil to criminal under the ITE Law and the P2SK Law.

2. Legal and Technical Risk Mitigation Framework
To provide robust legal certainty for capital market participants and prevent a legal vacuum resulting from technological vulnerabilities, a risk mitigation framework must be strictly integrated through OJK regulations. This is to be achieved through the implementation of the technical provisions of OJK Regulation (POJK) Number 27 of 2024 concerning the Conduct of Digital Financial Asset Trading—including Crypto Assets—as updated by OJK Regulation (POJK) Number 23 of 2025. This regulation serves as the primary foundation requiring providers of digital infrastructure in the financial market to implement information technology governance principles characterized by adaptability, transparency, and integrity.

Looking ahead, the OJK plays a pivotal role in expanding the scope of operational regulations for digital capital markets—extending beyond crypto assets to encompass the codification of technical rules for the tokenization of commodity-backed securities and financial instruments. This is reinforced by PADK 3/2026, the latest compliance instrument, which mandates periodic digital forensic audits, the use of regulatory sandbox mechanisms to test code resilience, and an ad-hoc electronic reporting system that must be activated immediately should an autonomous agent experience a cyber-related malfunction on the exchange. Through this hybrid supervisory approach, the OJK not only mitigates the risk of systemic functional failure but also proactively upholds consumer protection rights amidst the massive leap in the digitalization of the national capital market, namely:

a) Mechanism Emergency Circuit Breaker and Upgradeability Contract
Regulations governing digital capital markets must not permit smart contracts to operate with absolute immutability—entirely free from external oversight. From a technical standpoint, the code design must employ a proxy contract architecture to decouple state data storage from core business logic. Under this hybrid governance model, should transaction anomalies arise from cyberattacks or logic failures within the exchange's trading system, the OJK and KPEI—as holders of the multi-signature key—are empowered with the legal and technical authority to execute emergency intervention functions.[33] The requirement to establish an emergency halt mechanism (such as a circuit breaker or kill switch) is crucial for financial-sector smart contracts involving large-scale public transactions. This right of intervention enables a temporary digital suspension of trading and the application of code updates (patching) to safeguard investors' remaining assets; thus, the immutable nature of the code does not automatically preclude the enforcement of law and due process.[34]

b) Restructuring of the Mandatory Cyber Insurance Guarantee and Protection Fund
Amidst the disruption caused by decentralized technology, the conventional guarantee fund protection scheme managed by KPEI—acting as the Central Counterparty—requires a revolutionary overhaul. The traditional default waterfall structure, which currently relies on Clearing Member collateral and the Guarantee Reserve Fund, is deemed insufficient to mitigate the unique operational risks associated with cyber infrastructure. Consequently, the OJK, through its Financial Sector Technology Innovation cluster, must mandate that every blockchain-based stock exchange platform establish a strategic partnership with a specialized

[32] Javandalas Nanda Yasser Fatahillah Dkk, Analisis Hukum Keabsahan Kontrak Elektronik Sebagai Salah Satu Bentuk Kesepakatan Transaksi Elektronik Berdasarkan Perundang-Undangan Di Indonesia, *Amandemen: Jurnal Ilmu Pertahanan, Politik Dan Hukum Indonesia*, Vol. 2 No. 4 (2025), h. 1-12.

[33] Candra Wijaya Muling, Raul Gindo Cahayo, Dilema Code Is Law: Analisis Keadilan Kontraktual dan Perlindungan Hukum Bagi Pihak Lemah dalam Smart Contract, *Media Hukum Indonesia*, Vol. 4, No. 2, (2026), h 908-917.

[34] Van Vulpen, J., dkk. Defeasible Logic Reasoner to Support Legal Reasoning in Smart Contracts on Blockchain. *Frontiers in Blockchain*, 8(17), (2026). 1-15.

digital asset insurance provider. This third-party cyber insurance fund is projected to serve as a highly flexible "second-line liquidity cushion" capable of providing instant payouts. The instrument is crucial for recovering the tangible investment value of retail investors in the event of systemic technological failures—such as smart contract logic anomalies or protocol exploits—that fall outside the legal scope of conventional capital market risk protections. By strengthening these digital insurance regulations, the OJK not only reinforces the contemporary risk management architecture but also upholds comprehensive consumer protection pillars, thereby safeguarding stability and public confidence in the modern capital market ecosystem.[35]

c) Alignment of Investor Data Privacy Rights Based on Law Number 27 of 2022 concerning Personal Data Protection

The inherent characteristics of permanent transparency and data immutability in blockchain architecture inevitably give rise to a risk of legal conflict with the provisions of the Personal Data Protection (PDP) Law. This normative conflict centers on the fulfillment of a data subject's right to demand the destruction or deletion of their personal data—known as the "right to be forgotten" or "right to erasure" as guaranteed under Article 9 of the PDP Law—a requirement that is technically impossible to execute within a conventional distributed ledger.[36]

To mitigate such legal risks, the governance of digital capital market infrastructure must employ a hybrid architecture that prohibits the direct storage of investors' actual identity data on the blockchain (on-chain). The processing and storage of sensitive personal data must be shifted off-chain—managed centrally by KSEI—utilizing high-level encryption standards and strict access controls. Conversely, information recorded on the blockchain is limited to pseudonymized cryptographic hash representations. This technical approach ensures that exchange data remains secure and transparent for audit purposes without exposing investors' actual identities to the public, while simultaneously maintaining full compliance with the national data protection legal framework.[37]

d) Obligation to Undergo Feasibility Testing via the Financial Services Authority's Regulatory Sandbox

Before a smart contract protocol, securities tokenization, or Distributed Ledger Technology (DLT) platform is commercially deployed on the Indonesia Stock Exchange (IDX), the digital infrastructure must pass legal, technical, and operational feasibility tests via the OJK's regulatory sandbox mechanism. Pursuant to OJK Regulation (POJK) Number 3/2024, this controlled testing environment serves as a prudential filter to screen innovative financial business models before they obtain full operational licenses.[38] The implementation of this experimental phase is specifically designed to evaluate system reliability through structured external attack simulations, while also defining the parameters for civil liability risk mitigation to prevent transaction rejections caused by code logic flaws. By enforcing technical standards within this regulatory sandbox, the OJK exercises crucial oversight to ensure that the automation of decentralized instruments in the capital market operates in alignment with investor protection, market integrity, and the maintenance of national financial system stability.

From a doctrinal standpoint, civil liability for malfunctions in electronic systems or the destructive impact of cyberattacks on blockchain-based securities transactions must rest squarely with the stock exchange and the central securities depository—acting as Electronic System Providers (PSEs)—rather than with the abstract, decentralized computer network. This legal framework is firmly rooted in the mandate of Article 15, paragraph (1) of the ITE Law, which imperatively obliges PSEs to operate electronic systems reliably and securely, and holds them accountable for any losses arising during the system's operation. This liability regime is inherent and cannot be waived or transferred through unilateral exoneration clauses. The autonomous nature of blockchain technology must not serve as a legal shield or a ground for justification allowing exchange corporations and Self-Regulatory Organizations (SROs) to evade civil liability for financial losses suffered by retail clients. From the perspective of civil procedural law, computer networks, nodes, and lines of algorithmic code do not meet the fundamental criteria to qualify as legal subjects (*persona standi in judicio*); consequently, they cannot legally bear formal rights and obligations or be named as defendants in court proceedings.

Therefore, this cyber-autonomization must be strictly controlled through targeted technological modifications and mandatory regulatory interventions (*dwingend recht*). The doctrinal conflict between the immutable nature of decentralized technology and national legal certainty necessitates a shift by stock exchanges from a permissionless model to a permissioned ledger architecture that positions the regulator as the primary validator. Stock exchanges and central securities depositories must continue to act as ultimate guarantors to ensure the stability of the digital capital market, mitigate civil legal risks through the integration of Proxy Contracts, and uphold consumer protection pillars under Indonesian legal jurisdiction.

3. Conclusion

Based on the entire discussion and the legal analysis presented, this legal research formulates three main conclusions, as follows:

1. Normatively, smart contracts are valid and binding upon the parties (*verbindende kracht*) as an extension of Electronic Contracts under Article 1 point 17 and Article 18 paragraph (1) of the ITE Law. Their validity as admissible legal evidence in court proceedings is also explicitly affirmed by Article 44 paragraph (2) of the

[35] Hukumonline Newsroom. *Aturan Baru OJK, Penyelenggara ITSK dan Aset Digital Wajib Perkuat Tata Kelola*. Hukumonline Digital Journal (2025).

[36] Sihombing, R., dkk. Analisis yuridis penggunaan blockchain technology dalam ekosistem e-residency berkaitan dengan hak pelindungan data pribadi. *Jurnal Konsolidasi Hukum*, 7(1), (2025), h. 45–58.

[37] D. Kharisma, Pelindungan Data Pribadi Dalam Ekonomi Digital: Tantangan Implementasi Teknologi Blockchain di Indonesia. *Hukumonline Digital Economy Law Review*, 4(2), (2023). h. 112–129.

[38] Siti Azijah Alisia, Abdul Halim Barkatullah, Legalitas Bitcoin dan Teknologi Blockchain Dalam Sistem Keuangan Indonesia: Analisis Tatanan Hukum, *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol 3 No 3, (2025), h. 2856-2863.

P2SK Law. However, the self-executing and immutable characteristics of this technology trigger a tangible doctrinal conflict with conventional Indonesian contract law. Anonymous or pseudonymous transactions within decentralized systems potentially violate the subjective requirement of legal capacity set forth in Article 1320 of the Indonesian Civil Code. Furthermore, the rigidity of the program code inherently precludes the possibility of renegotiation and contravenes the doctrine of good faith and the traditional principle of consensualism in the event of market anomalies or *force majeure*.

2. The application of decentralization principles and distributed ledger technology has triggered radical institutional disruption within the Indonesian capital market. This autonomous, disintermediated blockchain mechanism directly challenges the monopolistic functions of KPEI and KSEI—functions otherwise protected by Articles 14 and 43 of the Capital Market Law. Shifting validation processes to global consensus algorithms creates a legal vacuum regarding the subject of civil liability while simultaneously deconstructing the traditional doctrine of liability based on fault. Nevertheless, this disruption offers efficiencies by eliminating single points of failure and enabling instantaneous—or T+0—transaction settlement.
3. In the event of an electronic system failure, code malfunction (logic bugs), oracle risk, or a structured cyberattack, civil liability rests absolutely with the stock exchange and the central securities depository acting as Electronic System Operators (Article 15 paragraph (1) of the ITE Law). The decentralized nature of blockchain must not be used as a legal shield to absolve corporations of the obligation to compensate clients for financial losses. Mandatory technical-legal risk mitigation measures include:
    a. Adoption of the Proxy Contract architecture to facilitate emergency intervention (circuit breaker) and code update (patching) functions by OJK and KPEI.
    b. Implementation of a permissioned ledger/hybrid blockchain architecture to ensure jurisdictional clarity and off-chain storage of personal data at KSEI, in order to comply with the "right to be forgotten" principle under the Personal Data Protection (PDP) Law.
    c. Specific digital cyber insurance obligation under OJK's ITSK regulations (POJK 3/2024) as a second-layer liquidity safety net to ensure the comprehensive enforcement of retail investor protection principles.

4. References

1. Arry Maulana Syarif, dkk. Blockchain: Konsep dan Arsitektur, Semarang, Ritecs, 2026.
2. Yofi Satriya Wijaya. Tinjauan Yuridis Peran PT Kliring Penjaminan Efek Indonesia Sebagai Central Counter Party Untuk Transaksi Derivatif Suku Bunga dan Nilai Tukar Over the Counter. Jurnal Dharmasisya. 2021; 1(3).
3. Aulia KS, Sitorus M, Batubara M. Peran Pasar Modal dalam Perekonomian Indonesia. JIKEM: Jurnal Ilmu Komputer, Ekonomi dan Manajemen. 2022; 2(2).
4. Kharisma D. Pelindungan Data Pribadi Dalam Ekonomi Digital: Tantangan Implementasi Teknologi Blockchain di Indonesia. Hukumonline Digital Economy Law Review. 2023; 4(2).
5. Szabo J, Bernard C, Philip L. Implications and Challenges of Blockchain Technology and Smart Contracts. Computer Life Journal (University of Kansas & University of Iowa School of Law). 2024; 12(2).
6. Babar A, Wu X. FinTech Transformations: Decentralized Automation and Technical Risks in Financial Sectors. Journal of Green FinTech and Financial Innovation. 2025; 14(1).
7. Deloitte Insights. Banking and Capital Markets Outlook: The Structural Shifts in Digital Asset Infrastructures. Financial Services Review, 2025.
8. Siswanto E, dkk. Reformasi Financial Flow melalui Tokenisasi Real World Asset (RWA): Analisis Desentralisasi dan Interoperabilitas Keuangan Global. Kajian Jurnal Manajemen dan Bisnis (KJMB). 2025; 3(2).
9. Fakhriah S, Hans SWP, Syamsul. Analisis Yuridis Keabsahan Smart Contract Dalam Perspektif Hukum Perdata Indonesia. Jurnal Kepastian Hukum dan Keadilan. 2025; 7(1).
10. Hukumonline Newsroom. Aturan Baru OJK, Penyelenggara ITSK dan Aset Digital Wajib Perkuat Tata Kelola. Hukumonline Digital Journal, 2025.
11. International Organization of Securities Commissions (IOSCO). Regulatory Models, Investor Protection, and Responsible Adoption in Digital Capital Markets. IOSCO Public Reports, ResearchGate Brief, 2025.
12. Javandalas Nanda Yasser Fatahillah, dkk. Analisis Hukum Keabsahan Kontrak Elektronik Sebagai Salah Satu Bentuk Kesepakatan Transaksi Elektronik Berdasarkan Perundang-Undangan di Indonesia, Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia. 2025; 2(4).
13. KPEI: Kliring & Penjaminan Transaksi Pasar Modal dan Inovasi Blockchain. INDODAX Academy Articles, 2025.
14. Maspul KA, Putri A. Teori digitalisasi pasar modal: Pengaruh digitalisasi terhadap efisiensi pasar keuangan. Journal of Innovative and Creativity. 2025; 1(1).
15. Monika Esterina Situmorang. Analisis Aspek Hukum Kontrak Pintar dalam Transaksi Kebendaan Digital: Tantangan Anonimitas dan Peran Identitas Digital, Lex Patrimonium. 2025; 4(1).
16. Nishith Desai Associates. Vulnerabilities in Smart Contracts and Cybersecurity Laws for Controllable Electronic Assets. Technical Law Review, Polymath Network Research Series, 2025.
17. Oxford Academic Cybersecurity. Reconciling Blockchain Technology and Data Protection Laws: Evolving Interpretations of Immutability and Joint Controllership. Cybersecurity Law Journal. 2025; 11(1).
18. Mukhlasin RM, Rahayu SAP. Transformasi hukum pasar modal di era digital: Pilar Investasi dan Pembangunan Ekonomi. YUSTISI. 2025; 12(3).
19. Sitorus RLO, dkk. Analisis Yuridis Keabsahan Smart Contract Sebagai Bentuk Perjanjian Elektronik di Indonesia. Jurnal Ilmiah Penelitian Mahasiswa (JIPM). 2025; 3(6).
20. Sihombing R, dkk. Analisis yuridis penggunaan blockchain technology dalam ekosistem e-residency berkaitan dengan hak pelindungan data pribadi. Jurnal Konsolidasi Hukum. 2025; 7(1).

21. Siti Azijah Alisia, Abdul Halim Barkatullah. Legalitas Bitcoin dan Teknologi Blockchain Dalam Sistem Keuangan Indonesia: Analisis Tatanan Hukum, Al-Zayn: Jurnal Ilmu Sosial & Hukum. 2025; 3(3).
22. Pratama AR. Menguji Asas Kebebasan Berkontrak Dalam Smart Contract. Journal of Electronic Research and Legal Innovation (JERKIN). 2026; 4(1).
23. Ana Tasia Pase. Perlindungan dan Kepastian Hukum Terhadap Transaksi e-Contract dalam Perjanjian Digital di Indonesia, Yustitiabelen. 2026; 12(2).
24. Bruegel Policy Brief. A new strategy to contain stablecoin risks in the European Union. Brussels Financial Studies Series, 2026.
25. Candra Wijaya Muling, Raul Gindo Cahayo. Dilema Code is Law: Analisis Keadilan Kontraktual dan Perlindungan Hukum Bagi Pihak Lemah dalam Smart Contract, Media Hukum Indonesia. 2026; 4(2).
26. Dimas Winky Siantu Setyo Negoro, dkk, Keabsahan Smart Contract Berbasis Blockchain Menurut Hukum Transaksi Perdagangan Indonesia, Al-Zayn: Jurnal Ilmu Sosial & Hukum. 2026; 6(1).
27. Darwis M, Hidayat R. Keabsahan dan Kekuatan Pembuktian Tanda Tangan Elektronik Pada Transaksi Bisnis Modern. Jurnal Mahkamah Hukum Islam (MHI). 2026; 4(1).
28. Financial Services Authority of Indonesia (OJK). Deepening Digital Financial Assets and Crypto Ecosystem Ecosystems. Press Release of OJK Annual Financial Industry Industry Meeting, 2026.
29. Fransisco W. Blockchain-based smart contracts: Legal certainty and regulatory implications within the Indonesian contract law framework. Jurnal Hukum dan Keadilan. 2026; 5(1).
30. Hacken Security Report. Q1 2026 Security & Compliance Report: Smart Contract Vulnerability Losses and Institutional Protocols Risk Mitigation. Hacken Compliance Docs, 2026.
31. Hapsari AW, Laia A. Kedudukan Hukum Smart Contract Dalam Sistem Perjanjian Menurut Hukum Perdata Indonesia. Jejak Digital: Indo Jurnal Press. 2026; 2(4).
32. Kurdi, dkk. Legal Analysis of Smart Contracts as Electronic Agreements under Civil and Electronic Transactions Law. Jurnal Hukum Magnum Opus. 2026; 9(1).
33. PwC Global Crypto Regulation Report. Regulatory Developments in Selected Jurisdictions for Capital Market Innovations. PwC Financial Services Network, 2026.
34. National Law Review. How Wall Street's Trillion-Dollar Crypto Infrastructure Push is Redefining Portfolio Diversification and Clearing Rail Systems. NLR Journal, 2026.
35. Harahap R, dkk. Tantangan Anonimitas dan Peran Identitas Digital dalam Implementasi Smart Contract Berbasis Blockchain. Jurnal Lex Patri. 2026; 14(2).
36. Ramli AF. Implikasi Perkembangan Teknologi Blockchain Terhadap Hukum Pembuktian Perdata di Indonesia. Jurnal Urusan Riset dan Inovasi Hukum (JURRISH). 2026; 2(1).
37. Sella S, dkk. Transformasi manajemen pasar modal di era digital. RIGGS: Journal of Artificial Intelligence and Digital Business. 2026; 5(2).
38. Sugiswati, *et al*. A Review of Civil Law Literature on Sales Contracts, Money Lending Agreements, and Smart Contract Integration for Indonesia Emas 2045. International Journal of Economic and Financial Issues. 2026; 6(2).
39. Van Vulpen J, dkk. Defeasible Logic Reasoner to Support Legal Reasoning in Smart Contracts on Blockchain. Frontiers in Blockchain. 2026; 8(17).