

Analysis of the Legal Framework of POJK 27/2024 Regarding Information Security for Crypto-Based Trading Assets

Dedi Gunawan,¹ Isman² Mariam El Banna³

^{1,2} Muhammadiyah University of Surakarta, Central Java, Indonesia

² Tantha University, Cairo, Egypt

¹ Corresponding Author: ism190@ums.ac.id
dg163@ums.ac.id

³ mariam.30917745@f-law.tanta.edu.eg

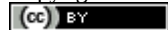
Submission Track:

Received: 10-06-2026

Final Revision: 06-08-2026

Available Online: 06-08-2026

Copyright © 2026 Authors



Abstract. This study analyzes OJK Regulation No. 27 of 2024 on Crypto Asset Trading from an information security perspective. Using normative legal research and a conceptual approach, the analysis draws on primary legal materials, including the regulation itself, and secondary materials, such as doctrine and literature. Through library research, the study employs a legal syllogism, using basic legal concepts legal subjects, objects of rights, legal relationships, juridical facts, and rights and legal obligations as the major premise, with normative facts from the regulation and privacy characteristics in the crypto ecosystem as the minor premise. The findings indicate that the regulation lacks a comprehensive legal framework, applying a uniform regime to crypto assets with varying privacy levels, from high Confidentiality to full transparency under Know Your Customer (KYC) principles. The absence of systematic differentiation among legal subjects, objects, relationships, and rights based on characteristics such as Confidentiality, Integrity, and Non-repudiation is evident. This research contributes that the systematic evaluation model, from the perspective of Legal Systematics Review, integrates the legal framework and the principles of Information Security as a tool for analyzing the quality of Crypto Asset Trading regulation in Indonesia. The normative framework includes privacy, traceability, authentication, authorization, and non-repudiation in each crypto technology. This means that the quality of POJK is not evaluated from the aspects of trading, governance, and market supervision, but also from its suitability with the information security characteristics that are the identity of each crypto asset.

Keywords: Legal Systematics Review; Crypto Asset Trading; Information Security

1 Introduction

The development of global digital financial instruments has driven a major transformation in the domestic regulatory landscape, one of which was triggered by comparative discourse regarding the application of crypto assets as commodities.¹ In Indonesia, regulatory authorities responded to this dynamic by shifting the oversight paradigm toward a single institution through the Financial Services Authority.² As a concrete step, the Financial Services Authority Regulation (POJK) Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading was issued.³ However, the basic character of this POJK is essentially highly administrative. The structure of the norms contained therein emphasizes the function of legal protection and the realization of stability in the financial system.⁴ The OJK strives for this stability by controlling the information system and strict licensing mechanisms for the main actors in the digital ecosystem, including the OJK itself, stock exchanges, clearing houses, storage facilities (custodians), and crypto asset traders.⁵ The OJK will only grant approval or operational permits when the information system proposed by these actors is proven to be knowable, controllable, and regulated in a structured manner.⁶ This administrative approach demands absolute harmony between written legal norms and the reliability of the technological infrastructure used.⁷

Technically, the security of these digital assets relies entirely on blockchain technology, which is driven by cryptographic functions, public and private key interactions, and dynamic *timestamp-based hash generation methods*.⁸ This interconnected data structure, like train carriages, creates a system that is resistant to tampering, as changing a single character will destroy the entire blockchain. This

¹ N Naifar and M S Makni, “Dynamics of Cryptocurrencies, DeFi Tokens, and Tech Stocks: Lessons from the FTX Collapse,” *International Journal of Financial Studies* 13, no. 3 (2025), <https://doi.org/10.3390/ijfs13030169>.

² R.I Otoritas Jasa Keuangan, “POJK Nomor 27 Tahun 2024,” Pub. L. No. 27 Tahun 2024 (2024).

³ F G Taştan, “Strict Liability of Crypto-Asset Service Providers: Turkish Law’s Sui Generis Response to MICA,” *European Review of Private Law* 33, no. 5–6 (2025): 1125–44, <https://doi.org/10.54648/erpl2025069>.

⁴ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

⁵ D Ahern, “Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon,” *European Business Organization Law Review* 22, no. 3 (2021): 395–432, <https://doi.org/10.1007/s40804-021-00217-z>.

⁶ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

⁷ L Hsu, “Digitalization and Its Role in International Economic Law,” *A Research: Agenda for Global Power Shifts and International Economic Law*, 2025, <https://doi.org/10.4337/9781035311507.00011>; A R Aruan, K Toha, and A R Nurdin, “Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities in Indonesia,” *APTISI Transactions on Technopreneurship* 7, no. 3 (2025): 1066–79, <https://doi.org/10.34306/att.v7i3.649>.

⁸ T I Iefymenko and T L Dmytrenko, “DEVELOPMENT AND INTEGRATION OF DIGITAL CURRENCIES IN THE VIRTUAL ASSET MARKET,” *Science and Innovation* 21, no. 2 (2025): 3–14, <https://doi.org/10.15407/scine21.02.003>; F Von Hafe et al., “Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe,” *Frontiers in Blockchain* 8 (2025), <https://doi.org/10.3389/fbloc.2025.1655230>.

complexity is further complicated by the decentralized and pseudonymous nature of transactions, meaning that transaction data is publicly available on a *peer-to-peer network*, but personally identifiable information remains hidden. This technical characteristic often creates a blind spot for legal scholars, as it produces *unidentified problems* that are difficult to address with conventional legal perspectives alone.⁹

A systematic legal analysis of POJK Number 27 of 2024 cannot be separated from *information security* and *privacy-based testing that preserves data mining*. The arrangement of the norm structure in POJK must be able to adopt and anticipate technical protocols for cybersecurity, data integration, and the risk of illegal use of computing resources, such as unauthorized.¹⁰ A legal system for digital financial legislation is considered ideal if the content of its norms is not only neat in an administrative-dogmatic manner but also fully compatible with mitigating vulnerabilities in the field's information technology architecture.¹¹ Based on this background, this systematic legal analysis research is directed at examining in depth the alignment between the juridical-administrative aspects and the technical aspects of cybersecurity.¹² The main focus of this research is whether POJK Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading, from an information security perspective, has a sound legal framework. The focus of this discussion is to determine the extent to which the OJK normative structure can bridge the blind spot between administrative legal regulations and blockchain security protocols to ensure the Integrity and stability of national finance.

2 Research Methods

This study uses a conceptual approach in a framework study of normative legal research, focused on systematic law.¹³ The conceptual approach is used to evaluate POJK Number 27 of 2024 concerning the Implementation of digital financial asset

⁹ Von Hafe et al., "Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe," 2025; L Pecis, L Cervi, and L Introna, "In Blockchain We Trust: Ideologies and Discourses Sustaining Trust in Bitcoin," *Information and Organization* 35, no. 2 (2025), <https://doi.org/10.1016/j.infoandorg.2025.100573>.

¹⁰ Y Gong, K P Chow, and S M Yiu, "Improved Bitcoin Simulation Model and Address Heuristic Method," *Forensic Science International: Digital Investigation* 53 (2025), <https://doi.org/10.1016/j.fsidi.2025.301935>; A Zimba et al., "Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security," *Journal of Computer Information Systems* 60, no. 4 (2020): 297–308, <https://doi.org/10.1080/08874417.2018.1477076>.

¹¹ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

¹² H M Sidik et al., "Harmonizing Gold-Backed Currencies Regulatory Framework in the Global Islamic Financial System," *Jurnal Hukum Islam* 23, no. 1 (2025): 229–64, <https://doi.org/10.28918/jhi.v23i1.08>; E Mik, "Why Should Contracts Be Smart?," *Private Law, Digital Assets, and Infrastructure*, 2025, https://doi.org/10.1007/978-981-96-7121-2_6.

¹³ I Isman and Ahmad Zainul Muttaqin, "Innovative Legal Modeling for Interdisciplinary Studies on Law and Economic Behavior," *Indonesian Journal of Islamic Economic Law* 1, no. 1 (December 7, 2023): 60–71, <https://doi.org/10.23917/ijoel.v1i1.3437>.

trading. It has formally met the conditions for a good law.¹⁴ Evaluation No done based on size substantive like justice, benefit, or certainty law, but rather based on definitions base in knowledge law consisting of on Legal Subject (subject) law), Object of Rights, Legal Relationship, Juridical Fact, as well as Rights and Legal Obligations.¹⁵ Through the approach, each draft law is made into a major premise with a method to describe the definition, characteristics, elements, scope, validity, and the differences with each other for formal size evaluation in systematic law regulation legislation.¹⁶

The legal materials used consist of primary and secondary law. Primary legal material in the form of POJK Number 27 of 2024 is the main object of research. In contrast, secondary legal material in the form of doctrines, literature, and concepts of law explains the understanding of the subject law, object law, relationship law, events law, as well as rights and obligations law. Data collection techniques for material law were: studies, library research, conducted research, and browsing legal sources and literature. In a study of systematic law, materials analysis is used to identify and inventory the content in referenced regulations, then group them based on a category that has been built through a major premise.¹⁷

Analysis method in material law use syllogism as a form of deductive reasoning.¹⁸ The major premise is arranged from concepts-based law obtained through doctrinal study regarding Legal Subject, Object of Rights, Legal Relationship, Juridical Fact, and Rights and Legal Obligations. The minor premise is arranged from facts, normative originating material primary and material secondary provisions in POJK Number 27 of 2024, which then are inventoried and described in a logical consistent manner deductive process, testing is conducted to determine the suitability between existing norms in POJK with elements of systematic law that becomes a formal measure of assessment, so a conclusion law about whether POJK Number 27 of 2024 has been own systematics good law or Still show structure laws that have not been systematic in a way holistic.¹⁹

3 Result and Discussion

The discussion in this paper is organized into four aspects. First, Crypto-Asset Trading and Systematic Review under POJK No. 27 of 2024 discusses the construction of normative trading assets in accordance with that POJK. Furthermore, Crypto-Asset

¹⁴ M Oderkerk, "Methods of Comparative Legal Research: How to Set up and Carry out a Comparative Legal Research Project," *Uncovering European Private Law A Student Handbook*, 2025, <https://doi.org/10.11647/OBP.0448.16>; KELIK WARDIONO et al., "Epistemology Of Legal Studies: Research Method Characteristics of Theoretical Law Bearers in Indonesia," *Journal of Ecohumanism* 3, no. 3 (June 24, 2024): 814–54, <https://doi.org/10.62754/joe.v3i3.3374>.

¹⁵ WARDIONO et al., "Epistemology Of Legal Studies: Research Method Characteristics of Theoretical Law Bearers in Indonesia."

¹⁶ Debasis Poddar, "Genealogy of Legal Research Methodology," *Asian Journal of Legal Education* 12, no. 2 (July 27, 2025): 121–37, <https://doi.org/10.1177/23220058251321027>.

¹⁷ Isman and Muttaqin, "Innovative Legal Modeling for Interdisciplinary Studies on Law and Economic Behavior."

¹⁸ Isman and Muttaqin.

¹⁹ WARDIONO et al., "Epistemology Of Legal Studies: Research Method Characteristics of Theoretical Law Bearers in Indonesia."

Trading and Systematic Literature Review presents a review of the literature on the characteristics of crypto assets and the development of their regulation. Third, Legal Systematics of Crypto-Assets and Information Security Principles carried out an analysis of the suitability of legal systematics, including Legal Subject, Object of Rights, Legal Relationship, Juridical Fact, as well as Rights and Legal Obligations, with information security principles, namely Confidentiality, Integrity, Availability, Authentication, Authorization, and Non-repudiation.

The fourth aspect is Developing Indonesian Crypto-Asset Trading Based on Information Security, which discusses the development of regulatory models for crypto-asset trading in Indonesia that are better aligned with the characteristics of information security. For strengthening analysis, discussion supported by several visualizations, namely Blockchain Mechanism, which explains how the blockchain mechanism works, Difference in Privacy Levels, which describes the spectrum of privacy levels on various crypto assets, as well as the Spectrum of Unsystematic POJK Structure, which shows the unsystematic structure of the POJK Law Number 27 of 2024 when connected with different characteristics of privacy and security information in the crypto asset ecosystem.

3.1 Crypto-Asset Trading and Systematic Review under POJK No. 27/2024

Literature reviews show that discussions on crypto assets are increasingly shifting from mere investment issues to information security as the foundation for implementing a crypto ecosystem.²⁰ Kerimov and Krasinsky found that the development of the crypto industry and digital assets is inseparable from the need to strengthen information security, as vulnerabilities in information infrastructure can undermine the stability of the digital financial system.²¹

Based on the general provisions of POJK Number 27 of 2024, legal subjects in the Crypto Asset trading ecosystem consist of regulators, organizers, business actors, and service users. The Financial Services Authority (OJK) is a public legal subject with the functions of regulating, supervising, inspecting, and investigating the Implementation of Digital Financial Asset activities, including Crypto Assets.²² Bappebti is also recognized as an institutional legal subject that previously had the functions of fostering, regulating, developing, and supervising futures trading.²³

²⁰ A I M Abdel-Razzaq and A Rafay, "From Collapse to Compliance: How Mt. Gox Shaped AI-Driven Governance of Digital Assets," *Financial Corruption and Money Laundering in the AI Era*, 2025, <https://doi.org/10.4018/979-8-3373-0786-2.ch001>; Von Hafe et al., "Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe," 2025.

²¹ A D Kerimov and V V Krasinsky, "DEVELOPMENT OF THE NATIONAL CRYPTO INDUSTRY AS ONE OF THE ELEMENTS OF THE FINANCIAL AND TECHNOLOGICAL SOVEREIGNTY OF THE STATE," *Gosudarstvo i Pravo* 2025, no. 2 (2025): 115–25, <https://doi.org/10.31857/S1026945225020111>.

²² Sidik et al., "Harmonizing Gold-Backed Currencies Regulatory Framework in the Global Islamic Financial System."

²³ Sidik et al.

Operationally, private legal subjects consist of the Stock Exchange, Clearing Guarantee and Settlement Institution, Depository Manager, Trader, Stock Exchange Member, Clearing Member, Main Party, Board of Directors, Board of Commissioners, and Consumer, each of whom obtains explicit legal standing in the general provisions of the POJK.²⁴ This means that the structure of legal subjects in this regulation is structured in layers, namely regulators, self-regulatory institutions, business actors, and users of Crypto Asset trading services.²⁵

The main legal object of focus regulated in POJK Number 27 of 2024 is Digital Financial Assets that are stored or represented digitally and include Crypto Assets as one form.²⁶ Crypto Assets are positioned as a digital representation of value that can be stored and transferred using distributed ledger technology such as blockchain to guarantee the validity and security of transactions.²⁷ In addition to Crypto Assets, other legal objects that are regulated are Wallets as a storage medium for Digital Financial Assets, Crypto Asset Lists as legal instruments for trading certain assets, Consumer funds placed in separate accounts, transaction data, ownership data, as well as systems and facilities for trading and storing Digital Financial Assets.²⁸

This means that the legal object of this regulation is not only digital assets as economic objects, but also includes data, electronic systems, storage infrastructure, and trading facilities that enable Crypto Asset transactions.²⁹ Viewed from a legal relationship perspective, this regulation designs a reciprocal legal relationship between the rights and obligations of legal subjects. Exchange members have the right to use the systems and facilities provided by the Exchange in accordance with Exchange regulations and rules after obtaining permission from the OJK.³⁰ Clearing members have the right to obtain transaction settlement services and transaction settlement guarantees from the Clearing, Guarantee and Settlement Institution.³¹

On the other hand, the Clearing Guarantee and Settlement Institution has an obligation to provide a reliable system, guarantee the settlement of transactions, monitor Consumer funds, maintain the Confidentiality of financial information, document all transaction data, and ensure the settlement of the parties' rights and obligations in the event of a default.³² The Storage Place Manager is also obliged to provide a safe, reliable, accountable storage system and guarantee the security of storage and transfer of Consumer Digital Financial Assets.³³

The OJK Regulation establishes a mutually integrated legal relationship between all legal subjects in the Crypto Asset trading ecosystem. The regulatory legal relationship

²⁴ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

²⁵ George Yudistira Irawan and Hwian Christianto, "Legal Regulations on Gold Banks Post-UUP2SK and POJK17/2024: Normative Review and Comparison with International Practices," *Journal of Social Research* 4, no. 8 (2025), <https://doi.org/10.55324/josr.v4i8.2726>.

²⁶ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

²⁷ Otoritas Jasa Keuangan.

²⁸ Otoritas Jasa Keuangan.

²⁹ Otoritas Jasa Keuangan.

³⁰ Otoritas Jasa Keuangan.

³¹ Otoritas Jasa Keuangan.

³² Otoritas Jasa Keuangan.

³³ Otoritas Jasa Keuangan.

occurs between the OJK and all Digital Financial Asset Trading Providers through licensing, approval, supervision, audit, and reporting mechanisms.³⁴ The legal relationship for trading occurs between Traders and Consumers through the buying and selling of Crypto Assets in the Digital Financial Asset Market. The legal relationship for transaction settlement is established among Traders, Exchanges, and Clearing Guarantee and Settlement Institutions that ensure the Implementation of clearing and settlement.³⁵ The legal relationship for storage occurs between Traders, Storage Managers, and Consumers through the mechanism of storage, maintenance, supervision, and delivery of Digital Financial Assets. Thus, the legal relationship within the OJK is systematically structured as a chain of trading, settlement, storage, and supervision of Crypto Assets.³⁶

Legal events in POJK Number 27 of 2024 include any event that gives rise to legal consequences for the parties. Crypto Asset Trading is a legal event that gives rise to rights and obligations between Traders and Consumers. Settlement of trade transactions through the Clearing, Guarantee and Settlement Institution is also a legal event that results in the transfer of rights to Digital Financial Assets and transaction funds.³⁷ A breach of promise that results in the non-fulfillment of obligations by one of the parties is a legal event that requires the Clearing, Guarantee and Settlement Institution to ensure the settlement of the rights and obligations of the parties. In addition, the occurrence of TPPU, TPPT, and PPSPM constitutes a legal event that gives rise to the obligation of the organizer of Digital Financial Asset trading to supervise, report, and take preventive action.³⁸

The legal community established by POJK Number 27 of 2024 is a digital legal community comprising regulators, trade organizers, trade support institutions, business actors, and consumers, all bound within a single Digital Financial Asset trading system.³⁹ This legal community is not formed based on territorial relations, but rather based on ties to Digital Financial Asset trading activities carried out through electronic means.⁴⁰ The existence of the Stock Exchange, Clearing Guarantee and Settlement Institution, Storage Place Manager, Traders, and Consumers indicates the existence of a legal community that carries out economic, supervisory, storage, and transaction protection functions in the same digital ecosystem.⁴¹

³⁴ P Dylan-Ennis and A Brody, "Tending the Infinite Garden: Organizational Culture in the Ethereum Ecosystem," *Journal of Cultural Economy*, 2025, <https://doi.org/10.1080/17530350.2025.2558576>.

³⁵ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

³⁶ Otoritas Jasa Keuangan.

³⁷ OJK, "Penguatan Sektor Jasa Keuangan Dalam Menjaga Pertumbuhan Ekonomi: Laporan Kinerja OJK Tahun 2023," 2024, [https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan Tahunan OJK 2023_.pdf](https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan%20Tahunan%20OJK%2023_.pdf).

³⁸ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

³⁹ Otoritas Jasa Keuangan.

⁴⁰ Puji Astuti and Isman Isman, "Legal Systematics of Supervision of the Financial Services Authority and Its Implications for the Implementation of Law Number 4 of 2023" 1, no. 01 (2024): 342–53.

⁴¹ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

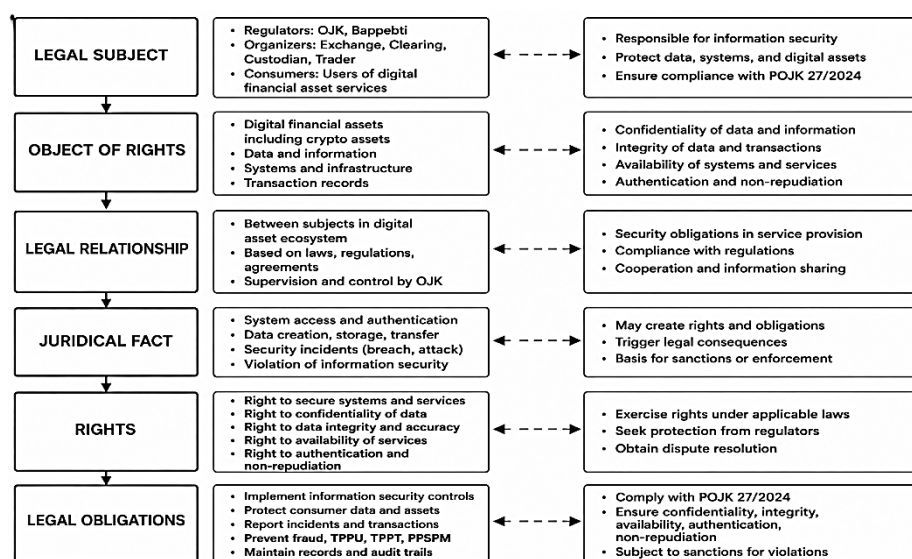


Fig. 1. Conceptual Legal Framework of POJK 27/2024

If all these elements are mapped systematically, POJK Number 27 of 2024 establishes a legal system comprising legal subjects, namely the OJK, the Stock Exchange, the Clearing Guarantee and Settlement Institution, Storage Place Managers, Traders, and Consumers. The legal objects are Digital Financial Assets, Crypto Assets, Wallets, Consumer funds, transaction data, and digital trading systems.⁴² The legal relationship is formed through trading, storage, clearing, guarantees, and transaction supervision. The legal events include trading, transaction settlement, asset storage, breach of contract, and actions related to TPPU, TPPT, and PPSPM. The rights and obligations of the parties are realized through trading systems, asset protection, transaction settlement, supervision of Consumer funds, and the maintenance of information security throughout the entire Crypto Asset trading cycle.⁴³

3.2 Crypto-Asset Trading and Systematic Literature Review

Literature reviews show that discussions on crypto assets are increasingly shifting from mere investment issues to information security issues, which serve as the foundation for implementing a crypto ecosystem.⁴⁴ Kerimov and Krasinsky found that the development of the crypto industry and digital assets cannot be separated from the need

⁴² Astuti and Isman, "Legal Systematics of Supervision of the Financial Services Authority and Its Implications for the Implementation of Law Number 4 of 2023."

⁴³ OJK, "Penguatan Sektor Jasa Keuangan Dalam Menjaga Pertumbuhan Ekonomi: Laporan Kinerja OJK Tahun 2023."

⁴⁴ A D Kerimov and V V Krasinsky, "DEVELOPMENT OF THE NATIONAL CRYPTO INDUSTRY AS ONE OF THE ELEMENTS OF THE FINANCIAL AND TECHNOLOGICAL SOVEREIGNTY OF THE STATE," *Gosudarstvo i Pravo* 2025, no. 2 (2025): 115–25, <https://doi.org/10.31857/S1026945225020111>.

to strengthen information security because vulnerabilities in information infrastructure have the potential to impact the stability of the digital financial system.⁴⁵

Similar findings were observed in Taştan's research, which showed that losses for crypto asset investors could arise from system failures, cyberattacks, information security breaches, and personnel errors by crypto asset service providers.⁴⁶ Meanwhile, Kushelevitch found that crypto asset activities require blockchain intelligence-based supervision to detect illegal transactions and maintain the Integrity of digital transactions⁴⁷.

When viewed through the lens of legal systematics, Taştan's research identifies Crypto-Asset Service Providers (CASPs) as legal subjects that provide crypto-asset services and bear responsibility for losses arising from information-security disruptions⁴⁸. Kushelevitch also identifies law enforcement officers and blockchain analysis companies as legal subjects involved in monitoring crypto-asset transactions⁴⁹. As for legal objects, Kerimov and Krasinsky identify cryptocurrency, virtual assets, and digital assets as objects that must be protected by strengthening information security in the digital financial system⁵⁰.

From a legal perspective, Taştan's research demonstrates a legal relationship between crypto asset service providers and investors that creates legal liability when losses result from system failures, cyberattacks, or information security breaches⁵¹. From a legal perspective, Kushelevitch identifies crypto-asset transactions used to finance terrorism as legal events that trigger investigations, blockchain tracking, and the seizure of digital assets by law enforcement⁵². From a rights and obligations perspective, Taştan's research demonstrates that crypto asset service providers have an obligation to ensure the system's operational security, as failure to fulfill this obligation can result in legal liability for service users⁵³.

If the literature study above is synthesized, it can be concluded that a consistent pattern is that information security is a fundamental need for managing crypto assets⁵⁴.

⁴⁵ Kerimov and Krasinsky.

⁴⁶ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁴⁷ M Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing," *Journal of Financial Crime* 32, no. 2 (2025): 403–15, <https://doi.org/10.1108/JFC-12-2023-0330>.

⁴⁸ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁴⁹ Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁵⁰ Kerimov and Krasinsky, "DEVELOPMENT OF THE NATIONAL CRYPTO INDUSTRY AS ONE OF THE ELEMENTS OF THE FINANCIAL AND TECHNOLOGICAL SOVEREIGNTY OF THE STATE," 2025.

⁵¹ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁵² Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁵³ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁵⁴ Kerimov and Krasinsky, "DEVELOPMENT OF THE NATIONAL CRYPTO INDUSTRY AS ONE OF THE ELEMENTS OF THE FINANCIAL AND TECHNOLOGICAL

Kerimov and Krasinsky emphasize the need to protect the information infrastructure to develop the national crypto industry⁵⁵. Tasthan identifies information security breaches as the basis for the emergence of legal liability for crypto asset service providers⁵⁶. Kushelevitch shows that blockchain analysis is an important instrument for information security in detecting and prosecuting illegal crypto-asset transactions⁵⁷. This pattern shows that information security has been understood as an operational and law-enforcement need in the crypto-asset ecosystem, but has not been positioned as a principle that underpins the structure of legal norms as a whole⁵⁸.

Therefore, the main components of crypto asset regulation are the actors involved in crypto transactions⁵⁹, objects in the form of cryptocurrency and digital assets⁶⁰, the legal relationship between service providers and users (Tasthan, 2025), legal events in the form of misuse and illegal transactions of crypto assets (Kushelevitch, 2025), and the obligation of organizers to maintain information system security (Tasthan, 2025). However, there has been no research that integrates all these elements into a systematic legal analysis that includes legal subjects, legal objects, legal relationships, legal events, and the rights and obligations of the parties in a normative framework based on information security (Kerimov & Krasinsky, 2025; Tasthan, 2025; Kushelevitch, 2025). The above findings can serve as a foundation for testing the legal systematics of POJK Number 27 of 2024, using information security as an integrative principle that connects all legal elements in the crypto asset investment ecosystem⁶¹.

Meanwhile, it is important to consider Kushelevitch's (2025) findings that the crypto asset ecosystem is always accompanied by the need to strengthen information security as the system's operational foundation. This is highly dependent on the effectiveness of crypto transaction monitoring, which in turn depends on the ability of blockchain

SOVEREIGNTY OF THE STATE," 2025; Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA"; Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁵⁵ Kerimov and Krasinsky, "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State," 2025.

⁵⁶ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁵⁷ Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁵⁸ Kerimov and Krasinsky, "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State," 2025; Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA"; Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁵⁹ S C Oranburg, "Function Over Form: Toward a Safe Harbor Framework for DeFi Regulation of Utility Tokens," *Louisiana Law Review* 86, no. 1 (2025): 81–166, <https://www.scopus.com/inward/record.uri?eid=2-s2.0-105032448070&partnerID=40&md5=31fa4aedcf1d8d6ec8b8315a18b52d31>.

⁶⁰ Kerimov and Krasinsky, "DEVELOPMENT OF THE NATIONAL CRYPTO INDUSTRY AS ONE OF THE ELEMENTS OF THE FINANCIAL AND TECHNOLOGICAL SOVEREIGNTY OF THE STATE," 2025.

⁶¹ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA"; Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

analysis and digital intelligence to detect illegal activity within the crypto asset network⁶². Meanwhile, Kerimov and Krasinsky (2025) position information security as a strategic element in the development of the crypto industry because it is linked to the legal responsibility of crypto asset service providers in the event of system failures, cyberattacks, or information security breaches⁶³.

Tastan's findings on Crypto-Asset Service Providers (CASPs) as legal entities responsible for user losses arising from information security breaches (Tastan, 2025). Other actors, according to Kushelevitch, are law enforcement officials, blockchain analysis companies, and crypto asset users⁶⁴. Meanwhile, cryptocurrencies and digital assets require protection in the digital financial system⁶⁵.

The literature review above concludes that studies on blockchain, encryption, authentication, and data security show that information security is more often positioned as a technical instrument than as a principle for the formation of legal norms. Sarfaraz (2021) emphasizes the importance of security, privacy, and cryptography in blockchain architecture to ensure the Integrity of digital transactions⁶⁶. Samy (2021) identifies authentication, identity confidentiality, and data protection as the main objectives of information security systems in the digital environment⁶⁷. Even research on ransomware and crypto-mining attacks focuses more on threat identification and cybersecurity risk mitigation mechanisms⁶⁸.

Another convergence is evident in the recognition across almost all studies that crypto asset activity occurs in an environment entirely dependent on the reliability of the information infrastructure. Kerimov and Krasinsky assert that the stability of the crypto industry can affect the digital financial system as a whole⁶⁹. The success of a blockchain system depends on meeting the security, privacy, and efficiency requirements of cryptography⁷⁰. Meanwhile, the increasing involvement of financial

⁶² Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁶³ Taştan, "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA."

⁶⁴ Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁶⁵ A Karminsky and M Stolbov, *Systemic Financial Risk: An Emerging Market Perspective*, 2024, <https://doi.org/10.1007/978-3-031-54809-3>.

⁶⁶ A Sarfaraz, R K Chakraborty, and D L Essam, "A Tree Structure-Based Improved Blockchain Framework for a Secure Online Bidding System," *Computers and Security* 102 (2021), <https://doi.org/10.1016/j.cose.2020.102147>.

⁶⁷ M M Samy et al., "An Optimized Protocol of M2M Authentication for Internet of Things (IoT)," *International Journal of Computer Network and Information Security* 13, no. 2 (2021): 29–38, <https://doi.org/10.5815/IJCNIS.2021.02.03>.

⁶⁸ A Zimba, Z Wang, and M Chishimba, "Addressing Crypto-Ransomware Attacks: Before You Decide Whether To-Pay or Not-To," *Journal of Computer Information Systems* 61, no. 1 (2021): 53–63, <https://doi.org/10.1080/08874417.2018.1564633>.

⁶⁹ Kerimov and Krasinsky, "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State," 2025.

⁷⁰ Kerimov and Krasinsky, "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State," 2025.

institutions in the digital asset market has made cybersecurity an integral part of their compliance and risk management strategies ⁷¹.

It can be concluded that the fundamental concepts for regulating crypto assets include the identification of actors, the characteristics of digital assets, the forms of legal relationships, transaction risks, oversight mechanisms, and legal liability arising from information security breaches ⁷². However, all of this research still moves partially in each aspect and has not built a conceptual bridge to a systematic legal analysis. As a result, there is still a gap in research regarding how legal subjects, legal objects, legal relationships, legal events, and the rights and obligations of the parties in POJK Number 27 of 2024 are constructed in an integrated manner based on information security principles.

3.3 Legal Systematics of Crypto-Assets and Information Security Principles

Based on blockchain operations as a collection of ledgers distributed across many points in a global network, so that stored information does not depend on one data center and cannot be unilaterally modified, because each ledger stores a copy of the same data ⁷³. From the perspective of systemic law, legal subjects comprise the perpetrators within the ecosystem, such as organizers, traders, storage managers, and consumers ⁷⁴. Object of Rights in the form of asset crypto along with recorded transaction data in the ledger ⁷⁵. Legal Relationships are formed when the subjects store, transfer, or trade crypto assets through the blockchain network. Juridical Facts emerged when the transaction was recorded, verified, and accepted in a distributed ledger ⁷⁶. Rights and Legal Obligations are formed through confessions, right ownership, rights diversion, obligations, honor, validity, and note transactions recorded on the blockchain.⁷⁷

Based on this mechanism, blockchain is a distributed recording infrastructure that connects legal subjects with the objects of their rights through legal relationships proven by legal facts in the form of transaction recordings on a ledger that cannot be

⁷¹ E Stavrova, "Banks' Digital Challenges," *Business Ethics and Leadership* 5, no. 3 (2021): 87–96, [https://doi.org/10.21272/bel.5\(3\).87-96.2021](https://doi.org/10.21272/bel.5(3).87-96.2021).

⁷² Kushelevitch, "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing."

⁷³ A.R. Kavitha, C. Sankari, and S. Angelus Ponmalar, "Decentralized Digital Ledger for Secure and Transparent Crypto Voting," in *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (IEEE, 2025), 1–7, <https://doi.org/10.1109/ICDSAAI65575.2025.11011783>.

⁷⁴ Francisco Von Hafe et al., "Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe," *Frontiers in Blockchain* 8 (August 6, 2025), <https://doi.org/10.3389/fbloc.2025.1655230>.

⁷⁵ Rainer Alt and Max Gräser, "Distributed Ledger Technology," *Electronic Markets* 35, no. 1 (December 11, 2025): 53, <https://doi.org/10.1007/s12525-025-00784-w>.

⁷⁶ A K Tyagi, "Advanced Topics for Blockchain-Based Applications: Open Issues, Technical, Legal, and Research Challenges," *Artificial Intelligence Enabled Digital Twin for Smart Manufacturing*, 2025, <https://doi.org/10.1002/9781394303601.ch15>.

⁷⁷ Alt and Gräser, "Distributed Ledger Technology."

manipulated, thus becoming the basis for the Implementation of rights and obligations in the crypto asset ecosystem.

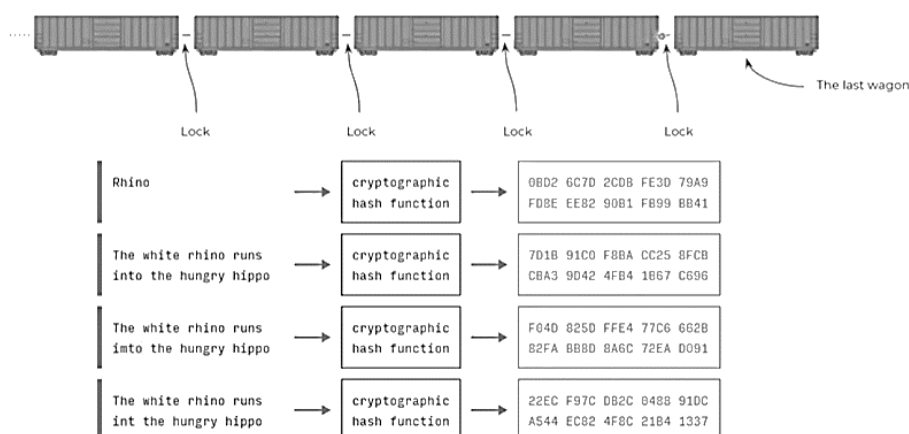


Fig. 2. Blockchain Mechanism ⁷⁸

Based on Figure 2 above, it can be concluded that blockchain operates as a series of interconnected blocks linked by a lock mechanism and a cryptographic hash function. Each block contains specific information, which is then processed through a cryptographic hash function to produce a unique digital identity ⁷⁹. The hash results serve as the link between one block and the next, so that the entire data series forms a continuous chain ⁸⁰. In the crypto asset ecosystem, this mechanism ensures that every action recorded on the blockchain is directly related to previous and subsequent actions. ⁸¹

Viewed from a juridical-fact perspective, the above mechanism shows that legal facts are formed on the blockchain once transaction data is input and processed through a cryptographic hash function ⁸². Before being input, transactions are just ordinary activities; after being recorded in a block and obtaining a specific hash, the transaction becomes a fact whose existence can be verified ⁸³. This means that recording a

⁷⁸ Hongyi Zhang et al., "Blockchain and Timely Auction Mechanism-Based Spectrum Management," *Future Generation Computer Systems* 166 (May 2025): 107703, <https://doi.org/10.1016/j.future.2024.107703>.

⁷⁹ Zhang et al.

⁸⁰ B Gayathri and V Vishwa Priya, "A Blockchain Network for Application for the Secure Goods and Services Tax Transaction Based on Hook Curve Revised Hash Authentication," *ITEGAM- Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA)* 12, no. 59 (2026): 182–94, <https://doi.org/10.5935/jetia.v12i59.3387>.

⁸¹ Gayathri and Priya.

⁸² Mingrui Qi and Dongdong Wang, "Secure Parallel Image Cryptographic Hash Function Using a Novel 2D High-Randomness Hyperchaotic Map," *Mathematics* 13, no. 11 (June 5, 2025): 1890, <https://doi.org/10.3390/math13111890>.

⁸³ Divyanshu Divyanshu et al., "Cryptographic Hash Function Using Current-Induced Magnetization Switching in Nano-Magnetic Devices," in *2025 IEEE International*

transaction in a block marks the transformation from a factual act into a legal fact with legal consequences in crypto assets.

The second legal event occurs when a block that already has a hash is linked to another block through a lock mechanism. The relationship between blocks indicates that legal facts (facts that give rise to rights and obligations) have been recorded so that they do not stand alone but rather become part of a continuous chronological sequence⁸⁴. Thus, the blockchain not only records transactions but also the sequence of events that form the history of the parties' activities in a continuous and traceable manner⁸⁵.

From a legal relationship perspective, the mechanism in Figure 2 above means that the relationship between the parties arises through the interconnectedness of data reflected on the blockchain⁸⁶. When a party performs an action recorded on the blockchain, that action generates data that becomes part of the same chain as the other party's actions. Consequently, the legal relationship is not formed solely by the parties' will but also by the existence of digital records that link their actions within the same blockchain system⁸⁷.

Symposium on Circuits and Systems (ISCAS) (IEEE, 2025), 1–5, <https://doi.org/10.1109/ISCAS56072.2025.11044006>.

⁸⁴ I Isman, Prima Ariyo Widodo, and R Risdayani, “Declining NPF Threatens Islamic Finance Stability: Unveiling Negative Correlation with CAR (2021-2023) through Robust Statistical Analysis,” *Proceeding ISETH (International Summit on Science, Technology, and Humanity)*, January 30, 2024, 2465–77, <https://doi.org/10.23917/iseth.5163>.

⁸⁵ A M Merfield, “The Future of Money — Seen from Above,” *Economic Anthropology* 12, no. 1 (2025), <https://doi.org/10.1002/sea2.12344>; A Civelli and L E Jackson, “Cryptocurrencies, Stocks, and Economic Policy Uncertainty: A FAVAR Analysis,” *North American Journal of Economics and Finance* 78 (2025), <https://doi.org/10.1016/j.najef.2025.102405>.

⁸⁶ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

⁸⁷ Qi and Wang, “Secure Parallel Image Cryptographic Hash Function Using a Novel 2D High-Randomness Hyperchaotic Map”; Zhang et al., “Blockchain and Timely Auction Mechanism-Based Spectrum Management”; Xinzhe Huang et al., “Dynamically Redactable Blockchain Based on Decentralized Chameleon Hash,” *Digital Communications and Networks* 11, no. 3 (June 2025): 757–67, <https://doi.org/10.1016/j.dcan.2024.10.013>; Gayathr and Priya, “A Blockchain Network for Application for the Secure Goods and Services Tax Transaction Based on Hook Curve Revised Hash Authentication.”

This legal relationship is strengthened because each block derives its validity from the previous block. This mechanism creates a chain-like connection between all recorded activities. In the context of crypto assets, this connection produces a chronologically traceable network of legal relationships, allowing each party's position in a transaction to be understood through the sequence of blocks stored in the blockchain⁸⁸.

Cryptocurrency	Privacy Level	Privacy by Default?	Main Technology
Monero (XMR)	★★★★★	Yes	RingCT, Stealth, Ring Signatures
Zcash (ZEC)	★★★★☆	No	zk-SNARKs
Dash	★★★★☆	No	CoinJoin-like
Bitcoin (Mixing)	★★☆☆☆	No	CoinJoin
Ethereum (Mixing/Stealth)	★★☆☆☆	No	zk-rollups (optional)
Litecoin	★★☆☆☆	No	MWEB
Solana / Cardano / BNB	★☆☆☆☆	No	Transparent
USDT / USDC / Stablecoins	★☆☆☆☆	No	Fully KYC + Transparent

Fig. 3. Difference in Privacy Levels⁸⁹

The principle of “Da Mihi Factum, Dabo Tibi Ius” is evident in the hash formation process in the image. Facts provided to the blockchain system in the form of transaction data are processed through a cryptographic hash function to produce a digital identity that is specific and different from other data⁹⁰. The hash functions as an objective representation of the facts that occurred⁹¹. With these recorded and verifiable facts, the

⁸⁸ C Carata and W J Knottenbelt, “The Economic and Geopolitical Implications of a U.S. National Bitcoin Reserve on Global Crypto Markets: Theoretical Underpinnings,” *Lecture Notes in Operations Research*, 2026, https://doi.org/10.1007/978-3-032-13377-9_16.

⁸⁹ Rakshith et al., “2LSS: A Two-Layer Security Scheme Using the Crypto-Steganography Approach to Enable High-Level Security for a Cloud Environment.”

⁹⁰ A Pagden, “Ius et Factum: Text and Experience in the Writings of Bartolomé de Las Casas,” *New World Encounters*, 2023, <https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85173368466&origin=inward>.

⁹¹ Divyanshu et al., “Cryptographic Hash Function Using Current-Induced Magnetization Switching in Nano-Magnetic Devices.”

basis for determining legal consequences becomes available, as the existence of facts no longer depends on unilateral recognition but on records stored on the blockchain.⁹²

Factual transaction data recorded in a block forms the basis for establishing legal relationships that can be traced through subsequent blocks. Thus, blockchain first presents transaction facts verified through hashes and locks, and then, from these transaction facts, legal relationships are formed between parties in the crypto ecosystem⁹³. Thus, blockchain functions as a mechanism that transforms transaction data into verifiable facts, and from these proven facts, sustainable legal relationships are formed within the crypto asset ecosystem.⁹⁴

To determine the security level of crypto asset transactions, Figure 3 above shows the differences in privacy levels (Difference in Privacy Levels) among various crypto assets, from Monero, which has the highest level of privacy, to highly transparent stablecoins. These differences directly influence the formation of legal relationships between crypto asset business actors, trade organizers, custodian providers, regulators, and consumers. The higher the level of Confidentiality, as in Monero and Zcash,⁹⁵ the more limited the identity and transaction information accessible to other parties.⁹⁶ Conversely, in more transparent systems such as Solana, Cardano, BNB⁹⁷, USDT,⁹⁸ and USDC⁹⁹, legal relationships are built through transparent transaction data, which facilitates the processes of Authentication, Authorization, and Non-repudiation.¹⁰⁰ Consequently, different levels of privacy result in varying degrees of ability for parties to prove identity, asset ownership, and transaction history in a legal relationship.¹⁰¹

⁹² Qi and Wang, "Secure Parallel Image Cryptographic Hash Function Using a Novel 2D High-Randomness Hyperchaotic Map."

⁹³ P Rakshith et al., "2LSS: A Two-Layer Security Scheme Using the Crypto-Steganography Approach to Enable High-Level Security for a Cloud Environment," *SN Computer Science* 7, no. 1 (December 26, 2025): 35, <https://doi.org/10.1007/s42979-025-04520-1>.

⁹⁴ Pagden, "Ius et Factum: Text and Experience in the Writings of Bartolomé de Las Casas."

⁹⁵ Azizah Binti Abdul Aziz et al., "Coinhive's Monero Drive-by Crypto-Jacking," *IOP Conference Series: Materials Science and Engineering* 769, no. 1 (February 1, 2020): 012065, <https://doi.org/10.1088/1757-899X/769/1/012065>.

⁹⁶ Cuneyt Gurcan Akcora, Yulia R. Gel, and Murat Kantarcioglu, "Blockchain Networks: Data Structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota," *WIREs Data Mining and Knowledge Discovery* 12, no. 1 (January 17, 2022), <https://doi.org/10.1002/widm.1436>.

⁹⁷ Jonathan Fior, "INNBC DApp, a Decentralized Application to Permanently Store Biomedical Data on a Modern, Proof-of-Stake (POS), Blockchain Such as BNB Smart Chain," *BMC Medical Informatics and Decision Making* 24, no. 1 (April 25, 2024): 109, <https://doi.org/10.1186/s12911-024-02498-z>.

⁹⁸ Musa Ayuba Musa and Temitope Akanbi, "Framework for the Adoption of Stablecoinss (USDT/BUSD) for Construction Payments," 2022, <https://doi.org/10.35490/EC3.2022.167>.

⁹⁹ Papa Ousseynou Diop and Julien Chevallier, "Binance USD Delisting and Stablecoins Repercussions: A Local Projections Approach," *Econometrics* 14, no. 1 (January 16, 2026): 6, <https://doi.org/10.3390/econometrics14010006>.

¹⁰⁰ Sajjad Alizadeh and Majid Khabbazi, "Solana's Transaction Network: Analysis, Insights, and Comparison," *EPJ Data Science* 14, no. 1 (July 14, 2025): 48, <https://doi.org/10.1140/epjds/s13688-025-00561-x>.

¹⁰¹ Junya Yamada et al., "On-Chain Analysis of Network Decentralization in Cardano Post-k Adjustment," in *2025 30th Asia-Pacific Conference on Communications (APCC)* (IEEE, 2025), 1–5, <https://doi.org/10.23919/APCC64555.2025.11279920>.

Every crypto asset transaction is an event that gives rise to legal consequences because it is recorded on the blockchain.¹⁰² However, Figure 3 above shows that the system's ability to reveal these legal facts varies depending on the level of privacy. In crypto assets with high privacy, legal facts remain and are recorded, but the Confidentiality mechanism limits access to the identity of the perpetrator and transaction details.¹⁰³ Conversely, in more transparent assets, legal facts can be verified more easily through the Integrity, Availability, and Authentication mechanisms because transaction data is more readily traceable.¹⁰⁴

As a legal consequence, the higher the level of privacy of a crypto asset, the greater the need for additional mechanisms to link the technical facts in the blockchain with the legal identities of the parties involved in the transaction.¹⁰⁵

Viewed from the perspective of Confidentiality, Integrity, Availability, Authentication, Authorization, and Non-repudiation, figure 3 above shows a trade-off between privacy protection and ease of legal proof.¹⁰⁶ A high level of privacy strengthens Confidentiality but can weaken other parties' ability to verify identity and prove transactions. Conversely, a low level of privacy strengthens Availability, Authentication, and Non-repudiation because data is easier to verify and trace.¹⁰⁷ The legal consequence (differences in privacy levels) is a different level of risk in the formation, Implementation, and proof of legal relationships.¹⁰⁸ The higher the privacy of a crypto asset, the greater the challenge for business actors and regulators in linking legal identity to transaction facts, while the more transparent a crypto asset, the stronger the position of legal proof regarding the rights, obligations, and responsibilities of parties in the crypto asset trading ecosystem.¹⁰⁹

¹⁰² Aditya Ahuja, Vinay Ribeiro, and Ranjan Pal, "How Should We Regulate Cryptocurrencies via Consensus?: A Strategic Framework for Optimal Legal Transaction Throughput," *Distributed Ledger Technologies: Research and Practice* 2, no. 1 (September 30, 2023): 1–20, <https://doi.org/10.1145/3567593>.

¹⁰³ J. Seol et al., "A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space," in *2025 7th International Conference on Blockchain Computing and Applications (BCCA)* (IEEE, 2025), 161–68, <https://doi.org/10.1109/BCCA66705.2025.11229817>.

¹⁰⁴ Seol et al.

¹⁰⁵ Bacelius Ruru et al., "The Impact of Crypto-Asset Utilization as Payment Instrument toward Rupiah as Legal Tender in Indonesia," *Journal of Central Banking Law and Institutions* 1, no. 1 (December 28, 2021): 141–80, <https://doi.org/10.21098/jcli.v1i1.6>.

¹⁰⁶ Asmae Azbeg et al., "Hybrid Blockchain and Edge AI Framework for Data Integrity in IoT-Based Healthcare Systems," 2026, 140–47, https://doi.org/10.1007/978-3-032-23035-5_13.

¹⁰⁷ Udit Agarwal et al., "Blockchain and Crypto Forensics: Investigating Crypto Frauds," *International Journal of Network Management* 34, no. 2 (March 7, 2024), <https://doi.org/10.1002/nem.2255>.

¹⁰⁸ Benjamin Larsen et al., "Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (IEEE, 2023), 1049–59, <https://doi.org/10.1109/TrustCom60117.2023.00146>.

¹⁰⁹ Larsen et al.

3.4 Developing Indonesian Crypto-Asset Trading Based on Information Security

Based on POJK Number 27 of 2024, legal subjects have been clearly identified through the categories of Digital Financial Asset Trading Organizers, which include Exchanges, Clearing, Guarantee and Settlement Institutions, Depository Managers, Traders, Consumers, the Financial Services Authority (OJK), the Board of Directors, the Board of Commissioners, and the Main Party. The legal objects have also been defined as Digital Financial Assets, Crypto Assets, transaction data, Wallets, and Consumer funds.¹¹⁰

However, when interpreted through the lens of findings from the information security literature, a gap in legal systematics is evident, as the POJK has not explicitly articulated the relationship between legal subjects and the principles of Confidentiality, Authentication, and Authorization as the basis for the parties' legal status.¹¹¹ The POJK does regulate the obligation to maintain the Confidentiality of financial position information, the use of authorization for Traders, the application of two authentication factors, and the unique identification of transactions, but all of these provisions are placed as operational technical requirements, not as normative elements inherent in the legal status of the parties in the crypto ecosystem.¹¹² As a result, the relationship between legal subjects and legal objects has not been established within an information security framework that systematically explains who has the right to access, verify, and control digital legal objects.¹¹³

POJK Number 27 of 2024 has regulated various legal relationships between Traders, Consumers, Exchanges, Clearing Guarantee and Settlement Institutions, and Depository Managers through transaction settlement mechanisms, fund separation, transaction supervision, asset storage, and guarantees of the rights and obligations of the parties.¹¹⁴ However, literature studies show that legal relationships in the global crypto ecosystem are built on the principles of Integrity, Availability, and Non-repudiation,¹¹⁵ because the validity of legal relationships is highly dependent on data integrity, system availability, and the inability of the parties to deny transactions that have been carried out.

¹¹⁰ Larsen et al.

¹¹¹ Roman Korolov et al., "Authentication and Authorization Method Based on McEliece Crypto-Code Construction," in *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (IEEE, 2024), 1–5, <https://doi.org/10.1109/ISMSIT63511.2024.10757296>.

¹¹² Korolov et al.

¹¹³ Larsen et al., "Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets."

¹¹⁴ Kaisei Kajita et al., "Continuous Group Key Agreement with Flexible Authorization and Its Applications," in *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics* (New York, NY, USA: ACM, 2023), 3–13, <https://doi.org/10.1145/3579987.3586570>.

¹¹⁵ Leonard Hill et al., "Compromising Insecure Crypto Implementations: A Deep-Learning Based Cryptosystem-Agnostic Testing Framework," in *2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)* (IEEE, 2024), 1–6, <https://doi.org/10.1109/ACDSA59508.2024.10467395>.

Meanwhile, in POJK 27 of 2024, these principles are set out as requirements for real-time recording, unique transaction identification, information system audits, disaster recovery centers, business continuity plans, and ten-year data retention. However, all of these are still scattered across various technical provisions and have not yet been formulated as a legal relationship structure that explains how arises change, terminate, or are terminated based on the fulfillment of Integrity,¹¹⁶ Availability,¹¹⁷ and Non-repudiation.¹¹⁸ This means that the dimensions of legal relationships and rights and obligations are still administrative-operational, not a legal system based on information security.

The most fundamental gap lies in the Juridical Fact dimension (Legal Event). POJK Number 27 of 2024 does recognize TPPU (money laundering), TPPT (money laundering), PPSPM (money laundering), transaction manipulation, unclear sources of funds, threats to storage systems, and security breaches as conditions that must be prevented or monitored.¹¹⁹ However, POJK does not systematically explain how a violation of Confidentiality, Integrity, Availability, Authentication, Authorization, or Non-repudiation becomes a legal event that gives rise to specific legal consequences for all legal subjects.¹²⁰

On the contrary, global literature identifies cyberattacks, information security breaches, system failures, blockchain tracing, and illegal transactions as the starting point for legal relations, legal accountability, investigations, and law enforcement.¹²¹ So, if information security is used as a legal systematic lens, then the Juridical Fact dimension is the dimension that most shows that POJK Number 27 of 2024 does not yet have a complete legal systematics, because legal events are still positioned as operational risks that must be managed,¹²² not as a normative foundation that connects in an integrated manner legal subjects, legal objects, legal relations, and the rights and obligations of the parties in the crypto asset ecosystem.¹²³

When POJK Number 27 of 2024 is compared with the findings on Difference in Privacy Levels, the POJK's legal system does not yet connect legal subjects and legal objects to different levels of Confidentiality, Authentication, and Authorization for each

¹¹⁶ Seol et al., “A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space.”

¹¹⁷ Seol et al.

¹¹⁸ Jin Sun et al., “Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS,” *IEEE Access* 8 (2020): 155145–55, <https://doi.org/10.1109/ACCESS.2020.3018816>.

¹¹⁹ Otoritas Jasa Keuangan, POJK Nomor 27 Tahun 2024.

¹²⁰ Alt and Gräser, “Distributed Ledger Technology”; Seol et al., “A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space”; Korolov et al., “Authentication and Authorization Method Based on McEliece Crypto-Code Construction”; Sun et al., “Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS.”

¹²¹ Deepsubhra Guha Roy and Satish Narayana Srirama, “A Blockchain-based Cyber Attack Detection Scheme for Decentralized Internet of Things Using Software-Defined Network,” *Software: Practice and Experience* 51, no. 7 (July 7, 2021): 1540–56, <https://doi.org/10.1002/spe.2972>.

¹²² Leonidas Sotiropoulos, “Smart Contracts and AI in Insurance,” 2026, 259–86, <https://doi.org/10.4018/979-8-3373-7996-8.ch008>.

¹²³ Hsu, “Digitalization and Its Role in International Economic Law.”

type of crypto asset. POJK 27 of 2024 treats all Crypto Assets as relatively uniform regulatory objects, while the findings on privacy levels show that Monero,¹²⁴ Zcash,¹²⁵ Bitcoin Mixing,¹²⁶ Ethereum Stealth,¹²⁷ and Stablecoins have different capacities for identity disclosure and information access. As a result, the Legal Subject–Object of Rights dimension does not yet have a normative classification that explains how access rights, user identification, and control over legal objects vary with the privacy level of the crypto asset used.

OJK Regulation Number 27 of 2024 recognizes that legal relationships are formed through trading, storage, transaction settlement, and use of crypto asset services, and recognizes legal facts through the existence of digital asset transactions traded in the Digital Financial Asset Market. However, blockchain construction reveals that legal facts *arise* when transactions obtain a cryptographic hash, are entered into a block, and are linked through a lock to the previous block, forming a verifiable chain of facts.

This means that the legal systematic gap lies in POJK 27 of 2024, which does not distinguish the legal consequences of different levels of privacy and the ability to prove legal facts. In transparent assets like USDT, USDC, Solana, Cardano, and BNB, the principles of Integrity, Availability, and Non-repudiation are relatively stronger because transactions can be traced and verified. In contrast to Monero and Zcash, legal facts remain on the blockchain, but the connection between transactions and the parties' legal identities becomes more difficult to prove. This means that the Legal Relationship–Juridical Fact aspect shows a systematic lack of clarity because POJK has not yet constructed a relationship between the level of privacy of crypto assets and the ability to establish, prove, and trace legal relationships.

¹²⁴ Binti Abdul Aziz et al., “Coinhive’s Monero Drive-by Crypto-Jacking.”

¹²⁵ Akcora, Gel, and Kantarcioglu, “Blockchain Networks: Data Structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota.”

¹²⁶ Akcora, Gel, and Kantarcioglu.

¹²⁷ E L Ledoux and N Smaili, “Cryptocurrency Frauds: The FTX Story,” *Journal of Financial Crime* 32, no. 3 (2025): 530–44, <https://doi.org/10.1108/JFC-01-2024-0022>.

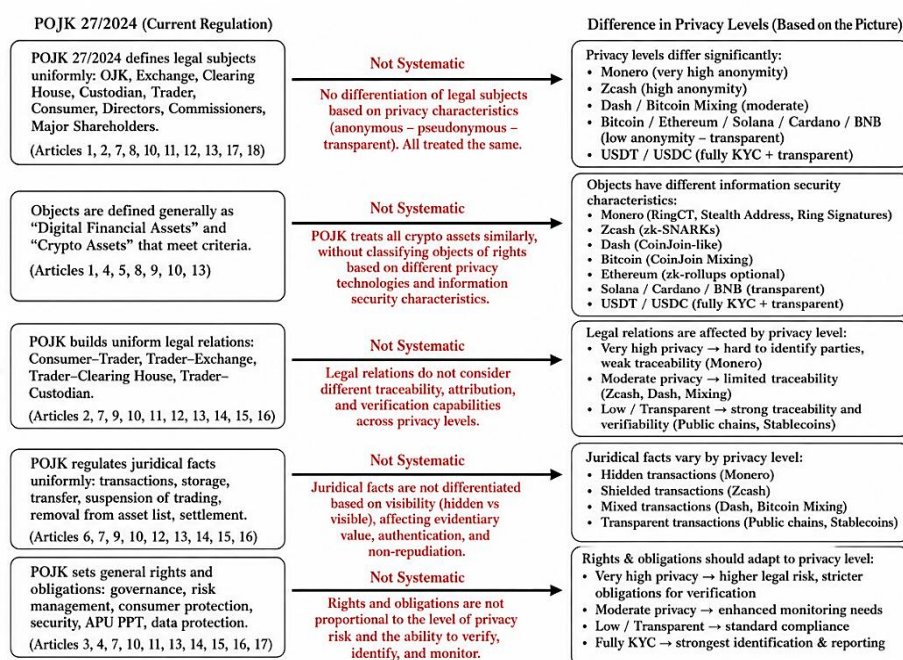


Fig. 3. Spectrum of Unsystematic POJK Structure

The largest gap lies in the Rights and Legal Obligations dimension. OJK Regulation No. 27 of 2024 grants Exchange Members, Clearing Members, and certain business actors the right to use facilitated systems and assigns oversight functions to the OJK and the organizers. However, the POJK has not yet structured the parties' rights and obligations around the principles of Confidentiality, Integrity, Availability, Authentication, Authorization, and Non-repudiation into a unified legal framework.

The Difference in Privacy Levels finding indicates that each type of crypto asset presents a different level of information security risk to proof of ownership, user identification, transaction monitoring, and legal liability tracing. If information security is used as an interpretive framework, the dimension that most clearly demonstrates that POJK Number 27 of 2024 lacks a fully clear legal system is the Rights and Legal Obligations dimension, as existing norms do not explicitly link the privacy levels of crypto assets to the rights, obligations, responsibilities, and legal proof mechanisms of the parties within the crypto asset ecosystem.

4 Conclusion

This study This study aims to answer whether POJK Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading is good w according to the information security perspective? Based on analysis to elements of Legal Subject, Object of Rights, Legal Relationship, Juridical Fact, and related Rights and Legal Obligations with Difference in Privacy Levels in the ecosystem crypto, found that POJK Number 27 of 2024 has not yet been have a systematic legal structure in a way

holistic, because build regime relative settings uniform to asset real crypto own characteristics security very different information, starting from from asset with very high level of Confidentiality like Monero to fully assets transparent and KYC- based like USDT and USDC. The most crucial finding that proves the unsystematic nature is the absence of a normative differentiation between subject law, object rights, relationships law, facts law, and rights and obligations law, based on the variation-level privacy, traceability, authentication, authorization, and non-repudiation inherent in each crypto technology. Findings: This is important because show that the arrangement asset crypto No Enough only oriented towards trade, governance, and market oversight, but must also be built based on characteristics of information security that become the identity of every type of asset crypto, so that can become runway conceptual formation or revision of the POJK in the future that is more adaptive to the development of blockchain technology and privacy-enhancing technologies. Research limitations: This is because the premise is minor and based on facts and normative sources from the POJK provisions and the characteristics of cryptotechnology, so the norm's operation in practice has not yet been tested. Furthermore, research needs to develop minor premise-based, empirically grounded facts through studies on trading assets and crypto, compliance mechanisms, the effectiveness of supervision, transaction investigations, consumer protection, as well as the Implementation of information security for crypto asset organizers in Indonesia.

REFERENCES

- Abdel-Razzaq, A I M, and A Rafay. "From Collapse to Compliance: How Mt. Gox Shaped AI-Driven Governance of Digital Assets." *Financial Corruption and Money Laundering in the AI Era*, 2025. <https://doi.org/10.4018/979-8-3373-0786-2.ch001>.
- Agarwal, Udit, Vinay Rishiwal, Sudeep Tanwar, and Mano Yadav. "Blockchain and Crypto Forensics: Investigating Crypto Frauds." *International Journal of Network Management* 34, no. 2 (March 7, 2024). <https://doi.org/10.1002/nem.2255>.
- Ahern, D. "Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon." *European Business Organization Law Review* 22, no. 3 (2021): 395–432. <https://doi.org/10.1007/s40804-021-00217-z>.
- Ahuja, Aditya, Vinay Ribeiro, and Ranjan Pal. "How Should We Regulate Cryptocurrencies via Consensus?: A Strategic Framework for Optimal Legal Transaction Throughput." *Distributed Ledger Technologies: Research and Practice* 2, no. 1 (September 30, 2023): 1–20. <https://doi.org/10.1145/3567593>.
- Akcora, Cuneyt Gurcan, Yulia R. Gel, and Murat Kantarcioglu. "Blockchain Networks: Data Structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota." *WIREs Data Mining and Knowledge Discovery* 12, no. 1 (January 17, 2022). <https://doi.org/10.1002/widm.1436>.
- Alizadeh, Sajjad, and Majid Khabbazzian. "Solana's Transaction Network: Analysis, Insights, and Comparison." *EPJ Data Science* 14, no. 1 (July 14, 2025): 48. <https://doi.org/10.1140/epjds/s13688-025-00561-x>.
- Alt, Rainer, and Max Gräser. "Distributed Ledger Technology." *Electronic Markets* 35, no. 1 (December 11, 2025): 53. <https://doi.org/10.1007/s12525-025-00784-w>.
- Aruan, A R, K Toha, and A R Nurdin. "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities in Indonesia." *APTISI Transactions on Technopreneurship* 7, no. 3 (2025): 1066–79. <https://doi.org/10.34306/att.v7i3.649>.
- Astuti, Puji, and Isman Isman. "Legal Systematics of Supervision of the Financial Services Authority and Its Implications for the Implementation of Law Number 4 of 2023" 1, no. 01 (2024): 342–53.
- Ayuba Musa, Musa, and Temitope Akanbi. "Framework for the Adoption of Stablecoinss (USDT/BUSD) for Construction Payments," 2022. <https://doi.org/10.35490/EC3.2022.167>.
- Azbeq, Asmae, Kebira Azbeq, Ouail Ouchetto, and Said Jai Andaloussi. "Hybrid Blockchain and Edge AI Framework for Data Integrity in IoT-Based Healthcare Systems," 140–47, 2026. https://doi.org/10.1007/978-3-032-23035-5_13.
- Binti Abdul Aziz, Azizah, Syahrulanuar Bin Ngah, Yau Ti Dun, and Tan Fui Bee. "Coinhive's Monero Drive-by Crypto-Jacking." *IOP Conference Series: Materials Science and Engineering* 769, no. 1 (February 1, 2020): 012065. <https://doi.org/10.1088/1757-899X/769/1/012065>.
- Carata, C, and W J Knottenbelt. "The Economic and Geopolitical Implications of a U.S. National Bitcoin Reserve on Global Crypto Markets: Theoretical Underpinnings." *Lecture Notes in Operations Research*, 2026.

- https://doi.org/10.1007/978-3-032-13377-9_16.
- Civelli, A, and L E Jackson. "Cryptocurrencies, Stocks, and Economic Policy Uncertainty: A FAVAR Analysis." *North American Journal of Economics and Finance* 78 (2025). <https://doi.org/10.1016/j.najef.2025.102405>.
- Diop, Papa Ousseynou, and Julien Chevallier. "Binance USD Delisting and Stablecoins Repercussions: A Local Projections Approach." *Econometrics* 14, no. 1 (January 16, 2026): 6. <https://doi.org/10.3390/econometrics14010006>.
- Divyanshu, Divyanshu, Aijaz H. Lone, Meng Tang, Daniel N. Rahimi, Selma Amara, and Gianluca Setti. "Cryptographic Hash Function Using Current-Induced Magnetization Switching in Nano-Magnetic Devices." In *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–5. IEEE, 2025. <https://doi.org/10.1109/ISCAS56072.2025.11044006>.
- Dylan-Ennis, P, and A Brody. "Tending the Infinite Garden: Organizational Culture in the Ethereum Ecosystem." *Journal of Cultural Economy*, 2025. <https://doi.org/10.1080/17530350.2025.2558576>.
- Fior, Jonathan. "INNBC DApp, a Decentralized Application to Permanently Store Biomedical Data on a Modern, Proof-of-Stake (POS), Blockchain Such as BNB Smart Chain." *BMC Medical Informatics and Decision Making* 24, no. 1 (April 25, 2024): 109. <https://doi.org/10.1186/s12911-024-02498-z>.
- Gayathri, B, and V Vishwa Priya. "A Blockchain Network for Application for the Secure Goods and Services Tax Transaction Based on Hook Curve Revised Hash Authentication." *ITEGAM- Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA)* 12, no. 59 (2026): 182–94. <https://doi.org/10.5935/jetia.v12i59.3387>.
- Gong, Y, K P Chow, and S M Yiu. "Improved Bitcoin Simulation Model and Address Heuristic Method." *Forensic Science International: Digital Investigation* 53 (2025). <https://doi.org/10.1016/j.fsidi.2025.301935>.
- Guha Roy, Deepsubhra, and Satish Narayana Srirama. "A Blockchain-based Cyber Attack Detection Scheme for Decentralized Internet of Things Using Software-Defined Network." *Software: Practice and Experience* 51, no. 7 (July 7, 2021): 1540–56. <https://doi.org/10.1002/spe.2972>.
- Hafe, F Von, Y Wagle, F Guede-Fernández, A P Giordano, L Silva, and S Azevedo. "Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe." *Frontiers in Blockchain* 8 (2025). <https://doi.org/10.3389/fbloc.2025.1655230>.
- Hafe, Francisco Von, Yash Wagle, Federico Guede-Fernández, Ana Paula Giordano, Luís Silva, and Salomé Azevedo. "Legal Frameworks for Blockchain Applications: A Comparative Study with Implications for Innovation in Europe." *Frontiers in Blockchain* 8 (August 6, 2025). <https://doi.org/10.3389/fbloc.2025.1655230>.
- Hill, Leonard, Florian Schimanke, Stefan Schiffner, and Robert Mertens. "Compromising Insecure Crypto Implementations: A Deep-Learning Based Cryptosystem-Agnostic Testing Framework." In *2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, 1–6. IEEE, 2024. <https://doi.org/10.1109/ACDSA59508.2024.10467395>.
- Hsu, L. "Digitalization and Its Role in International Economic Law." *A Research: Agenda for Global Power Shifts and International Economic Law*, 2025. <https://doi.org/10.4337/9781035311507.00011>.

- Huang, Xinzhe, Yujue Wang, Yong Ding, Qianhong Wu, Changsong Yang, and Hai Liang. "Dynamically Redactable Blockchain Based on Decentralized Chameleon Hash." *Digital Communications and Networks* 11, no. 3 (June 2025): 757–67. <https://doi.org/10.1016/j.dcan.2024.10.013>.
- Iefymenko, T I, and T L Dmytrenko. "Development And Integration Of Digital Currencies In The Virtual Asset Market." *Science and Innovation* 21, no. 2 (2025): 3–14. <https://doi.org/10.15407/scine21.02.003>.
- Irawan, George Yudistira, and Hwian Christianto. "Legal Regulations on Gold Banks Post-UUP2SK and POJK17/2024: Normative Review and Comparison with International Practices." *Journal of Social Research* 4, no. 8 (2025). <https://doi.org/10.55324/josr.v4i8.2726>.
- Isman, I, and Ahmad Zainul Muttaqin. "Innovative Legal Modeling for Interdisciplinary Studies on Law and Economic Behavior." *Indonesian Journal of Islamic Economic Law* 1, no. 1 (December 7, 2023): 60–71. <https://doi.org/10.23917/ijoe.v1i1.3437>.
- Isman, I, Prima Ariyo Widodo, and R Risdayani. "Declining NPF Threatens Islamic Finance Stability: Unveiling Negative Correlation with CAR (2021-2023) through Robust Statistical Analysis." *Proceeding ISETH (International Summit on Science, Technology, and Humanity)*, January 30, 2024, 2465–77. <https://doi.org/10.23917/iseth.5163>.
- Kajita, Kaisei, Keita Emura, Kazuto Ogawa, Ryo Nojima, and Go Ohtake. "Continuous Group Key Agreement with Flexible Authorization and Its Applications." In *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics*, 3–13. New York, NY, USA: ACM, 2023. <https://doi.org/10.1145/3579987.3586570>.
- Karminsky, A, and M Stolbov. *Systemic Financial Risk: An Emerging Market Perspective*. *Systemic Financial Risk: An Emerging Market Perspective*, 2024. <https://doi.org/10.1007/978-3-031-54809-3>.
- Kavitha, A.R., C. Sankari, and S. Angelus Ponmalar. "Decentralized Digital Ledger for Secure and Transparent Crypto Voting." In *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 1–7. IEEE, 2025. <https://doi.org/10.1109/ICDSAAI65575.2025.11011783>.
- Kerimov, A D, and V V Krasinsky. "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State." *Gosudarstvo i Pravo* 2025, no. 2 (2025): 115–25. <https://doi.org/10.31857/S1026945225020111>.
- . "Development Of The National Crypto Industry As One Of The Elements Of The Financial And Technological Sovereignty Of The State." *Gosudarstvo i Pravo* 2025, no. 2 (2025): 115–25. <https://doi.org/10.31857/S1026945225020111>.
- Korolov, Roman, Stanislav Milevskiy, Leonid Shcherbyna, Yana Lutsenko, Sergii Dunaiev, and Vadym Stetsenko. "Authentication and Authorization Method Based on McEliece Crypto-Code Construction." In *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 1–5. IEEE, 2024. <https://doi.org/10.1109/ISMSIT63511.2024.10757296>.
- Kushelevitch, M. "Unveiling the Crypto-Terror Nexus: Law Enforcement Intelligence Challenges against Terrorist Financing." *Journal of Financial Crime* 32, no. 2 (2025): 403–15. <https://doi.org/10.1108/JFC-12-2023-0330>.

- Larsen, Benjamin, Nada El Kassem, Thanassis Giannetsos, Ioannis Krontiris, Stefanos Vasileiadis, and Liqun Chen. "Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets." In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1049–59. IEEE, 2023. <https://doi.org/10.1109/TrustCom60117.2023.00146>.
- Ledoux, E L, and N Smaili. "Cryptocurrency Frauds: The FTX Story." *Journal of Financial Crime* 32, no. 3 (2025): 530–44. <https://doi.org/10.1108/JFC-01-2024-0022>.
- Merfield, A M. "The Future of Money — Seen from Above." *Economic Anthropology* 12, no. 1 (2025). <https://doi.org/10.1002/sea2.12344>.
- Mik, E. "Why Should Contracts Be Smart?" *Private Law, Digital Assets, and Infrastructure*, 2025. https://doi.org/10.1007/978-981-96-7121-2_6.
- Naifar, N, and M S Makni. "Dynamics of Cryptocurrencies, DeFi Tokens, and Tech Stocks: Lessons from the FTX Collapse." *International Journal of Financial Studies* 13, no. 3 (2025). <https://doi.org/10.3390/ijfs13030169>.
- Oderkerk, M. "Methods of Comparative Legal Research: How to Set up and Carry out a Comparative Legal Research Project." *Uncovering European Private Law A Student Handbook*, 2025. <https://doi.org/10.11647/OBP.0448.16>.
- OJK. "Penguatan Sektor Jasa Keuangan Dalam Menjaga Pertumbuhan Ekonomi: Laporan Kinerja OJK Tahun 2023," 2024. [https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan Tahunan OJK 2023_.pdf](https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan%20Tahunan%20OJK%2023_.pdf).
- Oranburg, S C. "Function Over Form: Toward a Safe Harbor Framework for DeFi Regulation of Utility Tokens." *Louisiana Law Review* 86, no. 1 (2025): 81–166. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-105032448070&partnerID=40&md5=31fa4aedcf1d8d6ec8b8315a18b52d31>.
- Otoritas Jasa Keuangan, R.I. POJK Nomor 27 Tahun 2024, Pub. L. No. 27 Tahun 2024 (2024).
- Pagden, A. "Ius et Factum: Text and Experience in the Writings of Bartolomé de Las Casas." *New World Encounters*, 2023. <https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85173368466&origin=inward>.
- Pecis, L, L Cervi, and L Introna. "In Blockchain We Trust: Ideologies and Discourses Sustaining Trust in Bitcoin." *Information and Organization* 35, no. 2 (2025). <https://doi.org/10.1016/j.infoandorg.2025.100573>.
- Poddar, Debasis. "Genealogy of Legal Research Methodology." *Asian Journal of Legal Education* 12, no. 2 (July 27, 2025): 121–37. <https://doi.org/10.1177/23220058251321027>.
- Qi, Mingrui, and Dongdong Wang. "Secure Parallel Image Cryptographic Hash Function Using a Novel 2D High-Randomness Hyperchaotic Map." *Mathematics* 13, no. 11 (June 5, 2025): 1890. <https://doi.org/10.3390/math13111890>.
- Rakshith, P, P Karthik, G Madhusudhan, K Ananya, and Nikhil Kangokar. "2LSS: A Two-Layer Security Scheme Using the Crypto-Steganography Approach to Enable High-Level Security for a Cloud Environment." *SN Computer Science* 7, no. 1 (December 26, 2025): 35. <https://doi.org/10.1007/s42979-025-04520-1>.
- Ruru, Bacelius, I Nyoman Tjager, Amalia Mayasari, Agradinda Adhistita, M. Raffi Hasta A., and August Santro. "The Impact of Crypto-Asset Utilization as Payment Instrument toward Rupiah as Legal Tender in Indonesia." *Journal of Central Banking Law and Institutions* 1, no. 1 (December 28, 2021): 141–80.

- <https://doi.org/10.21098/jcli.v1i1.6>.
- Samy, M M, W R Anis., A A Abdel-Hafez, and H D Eldemerdash. "An Optimized Protocol of M2M Authentication for Internet of Things (IoT)." *International Journal of Computer Network and Information Security* 13, no. 2 (2021): 29–38. <https://doi.org/10.5815/IJCNIS.2021.02.03>.
- Sarfaraz, A, R K Chakraborty, and D L Essam. "A Tree Structure-Based Improved Blockchain Framework for a Secure Online Bidding System." *Computers and Security* 102 (2021). <https://doi.org/10.1016/j.cose.2020.102147>.
- Seol, J., J. Deuja, Indy N. Park, Cong Pu, and N. Park. "A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space." In *2025 7th International Conference on Blockchain Computing and Applications (BCCA)*, 161–68. IEEE, 2025. <https://doi.org/10.1109/BCCA66705.2025.11229817>.
- Sidik, H M, W Santosa, M Dawud Arif Khan, and J K Kasuma. "Harmonizing Gold-Backed Currencies Regulatory Framework in the Global Islamic Financial System." *Jurnal Hukum Islam* 23, no. 1 (2025): 229–64. <https://doi.org/10.28918/jhi.v23i1.08>.
- Sotiropoulos, Leonidas. "Smart Contracts and AI in Insurance," 259–86, 2026. <https://doi.org/10.4018/979-8-3373-7996-8.ch008>.
- Stavrova, E. "Banks' Digital Challenges." *Business Ethics and Leadership* 5, no. 3 (2021): 87–96. [https://doi.org/10.21272/bel.5\(3\).87-96.2021](https://doi.org/10.21272/bel.5(3).87-96.2021).
- Sun, Jin, Xiaomin Yao, Shangping Wang, and Ying Wu. "Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS." *IEEE Access* 8 (2020): 155145–55. <https://doi.org/10.1109/ACCESS.2020.3018816>.
- Taştan, F G. "Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA." *European Review of Private Law* 33, no. 5–6 (2025): 1125–44. <https://doi.org/10.54648/erpl2025069>.
- Tyagi, A K. "Advanced Topics for Blockchain-Based Applications: Open Issues, Technical, Legal, and Research Challenges." *Artificial Intelligence Enabled Digital Twin for Smart Manufacturing*, 2025. <https://doi.org/10.1002/9781394303601.ch15>.
- Wardiono, Kelik, Khudzaifah Dimyati, Wardah Yuspin, Tasyha Panji Nugraha, Arief Budiono, And Saepul Rochman. "Epistemology Of Legal Studies: Research Method Characteristics of Theoretical Law Bearers in Indonesia." *Journal of Ecohumanism* 3, no. 3 (June 24, 2024): 814–54. <https://doi.org/10.62754/joe.v3i3.3374>.
- Yamada, Junya, Kentaroh Toyoda, Takanori Hara, Yu Nakahata, Christopher Wiraatmaja, and Shoji Kasahara. "On-Chain Analysis of Network Decentralization in Cardano Post-k Adjustment." In *2025 30th Asia-Pacific Conference on Communications (APCC)*, 1–5. IEEE, 2025. <https://doi.org/10.23919/APCC64555.2025.11279920>.
- Zhang, Hongyi, Mingqian Liu, Yunfei Chen, and Nan Zhao. "Blockchain and Timely Auction Mechanism-Based Spectrum Management." *Future Generation Computer Systems* 166 (May 2025): 107703. <https://doi.org/10.1016/j.future.2024.107703>.
- Zimba, A, Z Wang, and M Chishimba. "Addressing Crypto-Ransomware Attacks: Before You Decide Whether To-Pay or Not-To." *Journal of Computer*

- Information Systems* 61, no. 1 (2021): 53–63.
<https://doi.org/10.1080/08874417.2018.1564633>.
- Zimba, A, Z Wang, M Mulenga, and N H Odongo. “Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security.” *Journal of Computer Information Systems* 60, no. 4 (2020): 297–308.
<https://doi.org/10.1080/08874417.2018.1477076>.