

Juridical Analysis of Legal Protection for Cryptocurrency Investors Against Blockchain Risks under POJK 27/2024

Ahmad Imam Hambali,¹ Mahardi Arif,² Warda Said³, Andi Intan Purnamasari⁴

¹ Faculty of Law, Universitas Sebelas Maret, Surakarta, Central Java, Indonesia

² Chief of Crypto Investor, Medan, North Sumatra, Indonesia

³ Faculty of Law, Madako University, Tolitoli, Central Sulawesi, Indonesia

⁴ Andi Intan Purnamasari, National University of Malaysia, Kuala Lumpur, Malaysia

¹aih321@student.uns.ac.id

²risetmhes@gmail.com

³warda@umada.ac.id

⁴P131064@siswa.ukm.edu.my

Submission Track:

Received: 12-06-2026

Final Revision: 10-08-2026

Available Online: 11-08-2026

Copyright © 202x Authors



Abstract. This study examines how the Financial Services Authority Regulation (POJK) Number 27 of 2024 provides protection to cryptocurrency investors. This research focuses on how the regulations address blockchain risks such as cybersecurity threats, custodial issues, as well as rules that do not provide investors with a sense of security. This study uses a normative approach by analyzing blockchain regulations, as well as the methods used, such as interpretation and synthesis, to guide the analysis. The findings show that POJK Number 27 of 2024 provides a comprehensive legal framework for protection across governance, risk management, compliance, and law enforcement. The regulation provides legal protection in a juridical, preventive, and repressive manner. This research shows that protecting investors requires more than just the rule of law. Because blockchain risks are complex and cross-border, practical measures are needed, including stronger institutions and international cooperation. A major contribution from the study is the Integrative Legal Protection Model for the Blockchain Ecosystem, which integrates various legal protections to better protect cryptocurrency investors. This model emphasizes practical legal protections in addition to existing legal norms to address the challenges of blockchain technology.

Keywords: Cryptocurrency; Blockchain Risks; POJK; Legal Protection Model

1 Introduction

Development of blockchain technology has driven the growth of the cryptocurrency market at a global level as well as opened up opportunities for more and more retail investors to get involved in the world of digital finance. However, such increased participation is not always followed by an adequate understanding of the risks involved. Studies have shown that the complexity of blockchain systems, extremely high price fluctuations, the use of smart contracts, and the anonymous nature of transactions can put investors at risks that they often do not fully understand.

According to Lising, people who have low financial literacy and limited knowledge about blockchain are more likely to suffer losses when engaging in tokenization and cryptocurrency investments. This risk is even greater for groups with limited financial capabilities.¹ The situation is exacerbated by the emergence of various blockchain-based investment schemes that offer high returns, but also harbor threats such as security breaches, inadequate governance, market manipulation, and fraud.² This kind of risk is often difficult for investors who are just entering the world of digital assets. Therefore, the sustainability of the cryptocurrency ecosystem does not only depend on technological sophistication, but also on the existence of legal rules that are able to provide protection from blockchain risks.³

Judging from the legal aspect, the legal relationship between investors and crypto asset service providers is basically born from a contractual bond. Therefore, the relationship must be carried out by paying attention to the principles of legal protection, contract balance, good faith, information disclosure, and justice for all parties. Within a normative framework, digital finance regulations should be able to provide adequate rules regarding risk disclosure, prevention of conflicts of interest, protection of asset security, prohibition of misuse of investor funds, and clarity of responsibility when losses arise due to the failure of blockchain technology or digital intermediary services.⁴

POJK No. 27 of 2024 was issued as an effort to form digital financial asset governance that is able to provide legal certainty, protect consumers, and maintain market integrity. Conceptually, these regulations demonstrate the state's responsibility to provide an effective protection system against digital economy risks that are increasingly complex and beyond jurisdictional boundaries. Nevertheless, empirical findings show that there is still a considerable distance between the ideal or supposed legal provisions (*das Sollen*) and the reality of their implementation on the ground (*das Sein*). Recent literature indicates that blockchain risks stem not only from the price volatility of crypto assets but also from the technology's inherent characteristics, such as transaction anonymity, decentralization-based security, weaknesses in protocol governance, smart contract vulnerabilities, custodial failures, market abuse,

¹ P J L Lising, 'Reassessing Blockchain in Global Development: Tokenization of Infrastructure, Social Impacts, and the Axie Infinity Case in the Philippines', *Social Sciences and Humanities Open*, 13 (2026), doi:10.1016/j.ssaho.2025.102340.

² J Lee and L Schu, 'Market Abuse in the Cryptoassets Market: Same Risks, Same Activities, and Same Regulatory Outcomes?', *A Research Agenda for Financial Law and Regulation*, 2025, pp. 157–78, doi:10.4337/9781803929996.00015.

³ Lee and Schu.

⁴ A M Jaffri, 'Regulating Crypto Assets in the United States: Balancing Regulatory Effectiveness, Investor Protection, and Cross-Border Challenges', *Capital Markets Law Journal*, 21.2 (2026), doi:10.1093/cmlj/kmag015.

cryptojacking, money laundering mechanisms, and the difficulty in identifying the legal entity responsible for investor losses.⁵

The FTX case shows that weak governance and ineffective oversight systems can cause huge losses to investors, especially when their assets are lost in the absence of adequate recovery mechanisms.⁶ Meanwhile, a study on Axie Infinity shows that a token-based economic system has the potential to create a concentration of profits in certain groups. On the other hand, investors or users with more limited economic capabilities are more vulnerable to bear large losses due to ecosystem failures and token depreciation.⁷

Although blockchain is often introduced as a transparent technology that does not depend on trust in certain parties, its application actually raises various new legal risks that have not been fully accommodated in the investor protection system. The conflict between ideal investor protection norms and the reality of risk in the blockchain ecosystem raises a more fundamental legal issue, namely the lack of clarity regarding legal liability in the contractual relationship between investors and cryptocurrency platforms. The decentralized nature of blockchains, using pseudonyms, difficult to change, and supported by smart contracts makes the boundaries of responsibility between platforms, protocol developers, custodians, and users increasingly unclear.⁸

In addition, studies on cryptocurrency custodians show that the use of third-party custodial services can indeed provide convenience and increase technical security for users. However, the use of such services also presents new risks, especially related to the failure of intermediaries and the tendency of centralization that has the potential to harm investors.⁹ This condition confirms that the main issue in legal protection for crypto investors is not only related to technological risks, but also concerns how the law establishes legal relationships, divides responsibilities, and provides a compensation mechanism for losses incurred in the decentralized blockchain ecosystem.

A review of previous research shows that studies on cryptocurrencies can be grouped into several main categories. The first category discusses investor protection and regulation of the cryptocurrency market, with attention to the effectiveness of regulation, consumer protection, market integrity, as well as the governance of institutions or intermediaries in the cryptocurrency ecosystem.¹⁰ The second group examined the risks associated with blockchain technology, including system security, protocol governance, market abuse, money laundering mechanisms, and externalities

⁵ I Kokorin, 'The Decentralisation Defence', *Computer Law and Security Review*, 57 (2025), doi:10.1016/j.clsr.2025.106148.

⁶ E L Ledoux and N Smaili, 'Cryptocurrency Frauds: The FTX Story', *Journal of Financial Crime*, 32.3 (2025), pp. 530–44, doi:10.1108/JFC-01-2024-0022.

⁷ J Ali and G Vidan, 'Playing, Earning, Crashing, and Grinding: Axie Infinity and Growth Crises in the Web3 Economy', *Big Data and Society*, 12.3 (2025), doi:10.1177/20539517251357296.

⁸ A Didenko, 'Blockchain and Crypto-Assets', *Handbook of Blockchain in Public Governance*, 2026, pp. 219–31, doi:10.4337/9781035330096.00028.

⁹ A Carvalho, 'Cryptocurrency Custody', *Elgar Encyclopedia of Cryptocurrencies, Blockchain and DLT*, 2026, pp. 52–55, doi:10.4337/9781035339969.00016.

¹⁰ T Babenko and others, 'Risk Assessment of Cryptojacking Attacks on Endpoint Systems: Threats to Sustainable Digital Agriculture', *Sustainability (Switzerland)*, 17.12 (2025), doi:10.3390/su17125426.

generated by the blockchain ecosystem.¹¹ The third group discusses the legal and governance aspects of blockchain platforms from the perspectives of decentralization, smart contracts, transparency, and compliance-by-design.¹² Meanwhile, the fourth group examined investment risks and investor losses through case studies such as FTX, asset tokenization, the play-to-earn economy, stablecoins, and other crypto instruments.¹³ Methodologically, these studies are dominated by comparative normative approaches, case studies, systematic reviews, and interdisciplinary approaches grounded in technology and economics.

Although it has made a significant contribution to the development of the literature on crypto assets, prior research still leaves several gaps. Conceptually, existing research tends to frame blockchain risks primarily as issues of technology regulation, market governance, or compliance within the digital financial system, rather than as issues of investor legal protection arising from contractual relationships with crypto asset platforms.¹⁴

From a normative perspective, previous studies have not specifically examined how the concepts of rights, obligations, legal relationships, legal subjects, and investor liability are framed within the regulatory framework for cryptocurrency.¹⁵ Empirically, most research has focused on general blockchain risks, fraud, money laundering, or the failure of global platform governance, such as FTX, but has not thoroughly examined whether national regulatory frameworks are capable of anticipating the characteristics of blockchain risks stemming from anonymity, decentralization, and the lack of clarity regarding responsible parties.¹⁶

From a methodological perspective, no study has yet been identified that specifically employs a legal analysis of the structure of the investor-platform contractual relationship to assess the effectiveness of legal protections for cryptocurrency investors under POJK No. 27 of 2024.¹⁷ Given this gap, this study offers a novel approach in the form of a framework for analyzing legal protection for crypto investors based on contractual relationships, linking blockchain risks to the legal

¹¹ N Pocher, 'Traceability of Crypto-Asset Transfers under the New EU AML/ CFT Regime: The Crypto Travel Rule between Challenges and Open Issues', *A Research Agenda for Financial Law and Regulation*, 2025, pp. 197–219, doi:10.4337/9781803929996.00017.

¹² N Pocher, 'Crypto-Asset Ecosystems and the EU Anti-Money Laundering Framework: Law and Technology Perspectives', *Law, Governance and Technology Series*, 2025, 1–297, doi:10.1007/978-3-031-94698-1.

¹³ Y Cao and others, 'Designing Stablecoins', *Mathematical Finance*, 35.1 (2025), pp. 263–94, doi:10.1111/mafi.12445.

¹⁴ H M Sidik and others, 'Harmonizing Gold-Backed Currencies Regulatory Framework in the Global Islamic Financial System', *Jurnal Hukum Islam*, 23.1 (2025), pp. 229–64, doi:10.28918/jhi.v23i1.08.

¹⁵ T I Iefymenko and T L Dmytrenko, 'DEVELOPMENT AND INTEGRATION OF DIGITAL CURRENCIES IN THE VIRTUAL ASSET MARKET', *Science and Innovation*, 21.2 (2025), pp. 3–14, doi:10.15407/scine21.02.003.

¹⁶ A Tosato, D L Dick, and C K Odinet, 'DEBT TOKENS', *University of Pennsylvania Law Review*, 173.4 (2025), pp. 1103–71, doi:10.58112/uplr.173-4.3.

¹⁷ Tamiarisa Amanda Fasa Rambe and others, 'Kewenangan Badan Penyelesaian Sengketa Konsumen Kota Medan Memeriksa Sengketa Konsumen Jasa Keuangan Pasca Terbentuknya Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan', *Locus Journal of Academic Literature Review*, 1.2 (2022), pp. 109–16, doi:10.56128/ljoalr.v1i2.57.

concepts of legal subjects, legal objects, legal relationships, legal facts, rights, and obligations of the parties as outlined in POJK No. 27 of 2024.

Unlike previous studies that have focused on the regulation of cryptocurrencies in general, the risks of blockchain technology, or the governance of digital platforms, this study specifically examines how POJK No. 27 of 2024 establishes legal mechanisms to protect investors against blockchain risks, as well as the extent to which these regulatory provisions address issues of liability and investor compensation.

The objective of this study is to analyze the legal framework for protecting cryptocurrency investors from blockchain risks by conducting an in-depth examination of POJK No. 27 of 2024. The results of the study indicate that while POJK No. 27 of 2024 has established a foundation for investor protection through regulations governing digital asset operators, the regulation still leaves ambiguities regarding the allocation of responsibility for blockchain risks, such as its decentralized nature, transaction anonymity, and losses arising from ecosystem failures beyond the direct control of operators. This study is significant because it extends legal protection theory to blockchain-based contracting and provides a conceptual foundation for developing cryptocurrency regulations better adapted to the characteristics of decentralized technology and the need for investor protection in Indonesia.

2 Method

This study is a normative legal research project aimed at analyzing the legal protection framework for cryptocurrency investors in the face of blockchain risks through an in-depth examination of Financial Services Authority Regulation No. 27 of 2024 on the Conduct of Trading in Digital Financial Assets, including cryptocurrencies.¹⁸ Normative legal research was chosen because the focus of the study lies on the construction of legal norms, the systematics of regulations, the legal relationships between the parties, and the adequacy of regulations in protecting investors exposed to blockchain risks.¹⁹

The research approaches used are the statutory, conceptual, and case approaches. The statutory approach is used to examine the substantive alignment of POJK No. 27 of 2024 with the principles of legal protection, contractual justice, good faith, and consumer protection in the digital financial services sector.²⁰ The conceptual approach is used to analyze blockchain risk, legal liability, the crypto-asset ecosystem, and investor protection as they have evolved in the legal literature and in crypto-asset

¹⁸ A Perdana and others, *Digital Strategy and Governance in Transformative Technologies*, *Digital Strategy and Governance in Transformative Technologies*, 2025, doi:10.1201/9781003477808; 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)*, 2024, pp. 2465–77, doi:10.23917/iseth.5163.

¹⁹ V Belikoff and V Blazsek, 'A Systematisation of Legal-Regulatory Risks Related to Central Bank Digital Currencies: A Comparative Analysis of the US, the UK and China', *Law and Financial Markets Review*, 18.2 (2025), pp. 73–101, doi:10.1080/17521440.2025.2526326.

²⁰ Paulina E. Wilson, 'Comparative Law in Legal Education: An Interdisciplinary Perspective', *Juridical Tribune - Review of Comparative and International Law*, 14.3 (2024), pp. 345–62, doi:10.62768/TBJ/2024/14/3/01.

regulations. Meanwhile, the case approach is used to understand the empirical manifestations of blockchain risks by examining investor losses reported in the literature, including failures in crypto-platform governance, fraud, market abuse, transaction anonymity, and decentralization risks.²¹

The research data were obtained through library research using documentation techniques applied to primary, secondary, and tertiary legal materials. Primary legal materials include POJK No. 27 of 2024 and various regulations related to crypto assets. Secondary legal materials include articles from reputable international journals, books, handbooks, and research findings on investor protection, blockchain governance, cryptocurrency risks, smart contracts, crypto custody, and digital financial regulation. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting reference sources.

The data analysis in this study was carried out qualitatively through a prescriptive-analytical approach. The analysis process includes several stages, namely the collection and inventory of regulations, the grouping of legal issues, systematic interpretation, and the preparation of legal arguments. The main focus of the analysis is directed at efforts to find gaps between the investor protection provisions as stipulated in POJK No. 27 of 2024 and the characteristics of blockchain risks that emerge in practice. The findings of the analysis further became the basis for formulating a legal framework model for the protection of crypto asset investors that is more responsive to the development of blockchain technology as well as contractual relationships in the digital financial asset ecosystem.²²

3 Result and Discussion

This section is prepared to answer the main question of the extent to which the legal protection framework in POJK Number 27 of 2024 is able to respond to the risks inherent in blockchain-based ecosystems.²³ The analysis begins by identifying the various key risks of blockchain as discussed in the contemporary literature. The identification is used as an analytical basis in assessing the adequacy of applicable regulations.²⁴ Furthermore, this study examines the characteristics of legal protection contained in POJK Number 27 of 2024 to understand the scope and direction of investor protection provided by the regulation.²⁵

²¹ Henny Andriyani Wirananda, Wan Dian Safina, and Wilda Sri Munawaroh Harahap, 'The Role of Internal Control Over Sales, Receivables, Cash Receipts, and Cash Disbursements At Pt. Indako Trading Co', *Strategic Management Business Journal*, 2.02 (2022), pp. 99–104, doi:10.55751/smbj.v2i02.52.

²² S P Shapiro, 'Crypto Fever: Law, Regulation, and the Promise of Trustless Trust', *Annual Review of Law and Social Science*, 21.1 (2025), pp. 87–105, doi:10.1146/annurev-lawsocsci-110124-063008.

²³ R.I Otoritas Jasa Keuangan, *POJK Nomor 27 Tahun 2024* (2024).

²⁴ A Karminsky and M Stolbov, *Systemic Financial Risk: An Emerging Market Perspective*, *Systemic Financial Risk: An Emerging Market Perspective*, 2024, doi:10.1007/978-3-031-54809-3.

²⁵ Catrien Bijleveld, 'Methods for Empirical Legal Research', in *Digital Decade* (Nomos Verlagsgesellschaft mbH & Co. KG, 2025), pp. 21–40, doi:10.5771/9783748943990-21.

The next section discusses the relationship between the risks that arise in blockchain technology and the legal protection mechanisms available. This evaluation was carried out to assess the extent to which the existing regulatory framework is able to answer legal challenges stemming from technological developments. Furthermore, the findings are analyzed using legal protection theory to formulate a more comprehensive analytical framework for protecting cryptocurrency investors amid the dynamics of the blockchain ecosystem.

3.1 Blockchain Risk

POJK No. 27 of 2024 has established a framework for protecting crypto investors through regulations governing digital financial asset trading platforms, governance, risk management, and institution-based supervision. However, this study found that the substance of the legal protections established remains focused on institutional risk and has not yet fully accommodated the characteristics of blockchain risks that evolve dynamically within the decentralized finance (DeFi) ecosystem, asset tokenization, smart contracts, and cross-jurisdictional blockchain protocols. Consequently, there is a gap between the legal protection model established by regulators and the actual forms of loss faced by investors in modern blockchain networks.²⁶

Existing literature highlights risks related to wealth concentration and unequal benefit distribution within the blockchain ecosystem. Lising's (2026) analysis of infrastructure tokenization and the Axie Infinity case in the Philippines demonstrates that blockchain implementation does not necessarily ensure equitable distribution of benefits.²⁷ Lower and middle-income groups experience greater financial losses compared to investors with substantial capital. These findings indicate that blockchain risks encompass both technical and socio-economic dimensions. Under POJK No. 27 of 2024, there are currently no regulations that explicitly require operators to conduct social impact assessments or disclose information about potential profit concentration that may disadvantage retail investors.²⁸

Jaffri (2026) highlights that the global cryptocurrency market continues to face legal uncertainty due to divergent regulatory regimes across countries, contributing to regulatory arbitrage risk.²⁹ Indonesian investors transacting through blockchain-based platforms may be exposed to cross-border risks that are difficult for national jurisdictions to address. Although OJK Regulation No. 27 of 2024 has established obligations for operators under OJK supervision, it has not yet provided clear mechanisms for investor protection when losses arise from blockchain protocols or foreign entities outside Indonesian jurisdiction.³⁰

²⁶ C Zeiß and others, 'Exploring Trust in Decentralized Finance Intermediaries: A Taxonomy and Archetypes for Guiding Blockchain-Based Investment Decisions on the Web', *Internet Research*, 35.7 (2025), pp. 133–52, doi:10.1108/INTR-01-2025-0156.

²⁷ Lising.

²⁸ H. McNab and A. Wynn, *Principles and Practice of Consumer Credit Risk Management*, CIB Publishing, 2000.

²⁹ Jaffri.

³⁰ Refi Agustina and Fita Nurotul Faizah, 'Sharia Fintech: Opportunities and Challenges in Indonesia', *Journal of Islamic Economics (JoIE)*, 3.1 (2023), pp. 61–75, doi:10.21154/joie.v3i1.6289.

M Dhole et al (2026) highlight the risks of wallet fraud and the abuse of anonymous transactions developed a graph-based risk assessment model that identifies high-risk digital wallets through blockchain transaction analysis.³¹ The existence of this technology indicates that fraudulent activities, money laundering, and transaction manipulation can be detected through a blockchain forensics approach.³² However, POJK No. 27 of 2024 has not yet mandated the use of blockchain analytics technology as an investor protection tool. Consequently, preventive measures against risky transactions still depend on individual operators' policies.

The fourth finding indicates the emergence of increasingly complex money-laundering and scam-economy risks in the Southeast Asian region. A study by Dulisse et al. (2026) found that cryptocurrency has become a key financial infrastructure for organized fraud networks through the use of mixing services, privacy coins, and high-frequency transfers. These risks directly threaten investors by increasing the likelihood of indirect involvement in illegal activities that could lead to asset freezing. POJK No. 27 of 2024 adopts anti-money laundering principles, but it has not yet specifically regulated the evolving blockchain risk indicators on decentralized networks.

The finding by Carvalho (2026) highlights custody risk as one of the greatest risks in crypto investment and explains that investors face a dilemma between self-custody and third-party custody.³³ Self-custody provides full control over assets but increases the risk of losing private keys, whereas third-party custody poses the risk of a third party's failure. This study found that POJK No. 27 of 2024 regulates custodians more extensively than it addresses investor protection mechanisms in the event of asset loss due to blockchain technical errors or irrecoverable loss of cryptographic access.³⁴

Carvalho also identifies misleading investment intermediaries operating within the decentralized finance (DeFi) ecosystem, as many blockchain-based investment platforms offer unrealistic returns and low transparency.³⁵ The intricate nature of blockchain protocol governance presents challenges for investors in comprehending associated risks. From a legal protection standpoint, this study found that POJK No. 27 of 2024 has not established risk disclosure standards mandating that operators explain the characteristics of smart contracts, governance tokens, staking mechanisms, or decentralized finance (DeFi) protocol risks to investors.

The seventh finding reveals the risk of a "decentralization defense." Kokorin (2025) explains that decentralization is often invoked to avoid legal liability when investor losses occur.³⁶ The automatic execution of smart contracts makes it difficult to determine which party is responsible for system failures. This study found that POJK No. 27 of 2024 still assumes that there is always a legal entity that can be held accountable. However, in many blockchain protocols, developers, validators, DAOs, and users exist within a fragmented structure, creating a legal liability vacuum.

³¹ M Dhole and others, 'Crypto-Monitoring Tool', *Studies in Systems, Decision and Control*, 2026, 863–73, doi:10.1007/978-3-031-85398-2_76.

³² Y Gong, K P Chow, and S M Yiu, 'Improved Bitcoin Simulation Model and Address Heuristic Method', *Forensic Science International: Digital Investigation*, 53 (2025), doi:10.1016/j.fsidi.2025.301935.

³³ Carvalho.

³⁵ S C Oranburg, 'Function Over Form: Toward a Safe Harbor Framework for DeFi Regulation of Utility Tokens', *Louisiana Law Review*, 86.1 (2025), pp. 81–166.

³⁶ Kokorin.

The eighth finding highlights the risks of Ponzi-like tokenomics in blockchain gaming and play-to-earn systems. De Souza et al. (2025) found that game mechanics, token value, and withdrawal barriers are important signs of Ponzi-like schemes.³⁷ Ali and Vidan (2025) support these results, showing that when Axie Infinity's token value collapsed, investors and players suffered major losses. A normative analysis shows that POJK No. 27 of 2024 still fails to establish legal standards for assessing the sustainability of a blockchain project's tokenomics before it is marketed to investors.³⁸

Ledoux and Smaili (2025) found that FTX collapsed primarily due to governance failures, conflicts of interest, and weak internal oversight. This example shows that blockchain technology does not automatically protect investors. While POJK No. 27 of 2024 regulates governance obligations, it does not establish oversight standards that include proof of reserves, real-time audits, or blockchain transparency checks to protect investors.³⁹

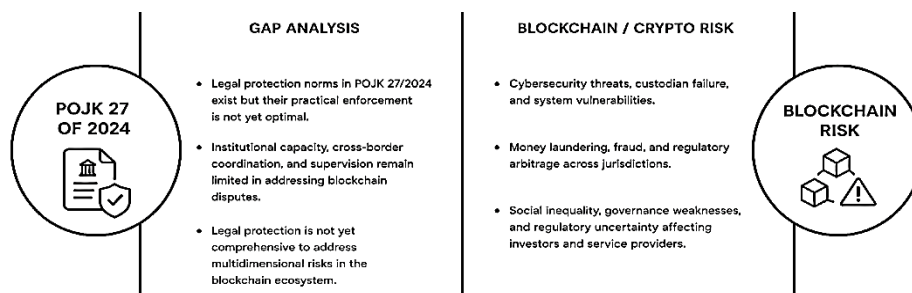


Fig. 1. Gap Analysis: POJK 27 of 2024 and Blockchain Risk

Lee and Schu (2025) found that wash trading, pump-and-dump schemes, front-running, and smart contract-based manipulation represent new forms of market abuse within the crypto ecosystem. These risks are not entirely identical to those of manipulation in conventional capital markets because they are carried out automatically by program code. This study found that POJK No. 27 of 2024 has not yet developed an algorithm-based supervisory approach capable of detecting market manipulation in real-time within blockchain networks.⁴⁰

Pocher (2025) explains that the implementation of the crypto travel rule faces a conflict between the need for traceability for AML/CFT and the protection of user privacy. This risk is further heightened with the use of self-hosted wallets and privacy-enhanced protocols. Within the framework of POJK No. 27 of 2024, it was found that the regulation places greater emphasis on transparency and reporting but has not yet

³⁷ P V S de Souza, R S Lima, and R B Almeida, 'Red Flags in Play-to-Earn Crypto Games: Proposal and Testing of a Checklist Based on Ponzi Scheme', *Revista de Contabilidade e Organizações*, 19 (2025), doi:10.11606/issn.1982-6486.rco.2025.230807.

³⁸ Otoritas Jasa Keuangan.

³⁹ Otoritas Jasa Keuangan.

⁴⁰ B C Dulisse, J Denis, and N Connealy, 'Exploring the Extent of International Money Laundering Using Cryptocurrency: A Systematic Scoping Review of Gaps in Research on Southeast Asia's Scam Economy', *Journal of Money Laundering Control*, 2026, pp. 1–19, doi:10.1108/JMLC-12-2025-0241.

detailed provisions that address the balance between protecting investors' personal data and the need for blockchain transaction oversight.⁴¹

Martino and Ringe (2025) assert that blockchain poses operational, legal, governance, and external risks that cannot be resolved solely through decentralized mechanisms. Based on an analysis of POJK No. 27 of 2024, this study concludes that the legal framework for protecting crypto investors in Indonesia remains oriented toward an intermediary-based regulatory approach. Meanwhile, various risks associated with modern blockchain actually stem from the technology's inherent characteristics, such as immutability, pseudonymity, decentralization, smart contract automation, tokenomics failure, and cross-border architecture. Therefore, a reformulation of investor legal protection is needed to establish a blockchain risk-based regulatory framework that comprehensively integrates legal, technological, governance, cybersecurity, algorithmic transparency, and investor protection aspects.⁴²

3.2 Characteristics of Legal Protection of POJK 27 of 2024

The first characteristic of POJK 27 of 2024 is a system-security-based preventive legal protection model. This characteristic is evident in the obligation of Storage Facility Operators to provide a system that is accurate, secure, reliable, compatible, and capable of safeguarding the security of the storage and transfer of consumers' Digital Financial Assets. The regulation does not wait for investor losses to occur; instead, it establishes preventive mechanisms at the design stage of the storage infrastructure. Thus, legal protection is positioned as a risk prevention instrument for blockchain before disputes or investor losses arise.

The second characteristic demonstrates that POJK No. 27 of 2024 adopts a cyber-risk preventive-protection model. The mandate for a disaster recovery centre, a business continuity plan, and adherence to international information security standards suggests that investor protection extends beyond formal legal considerations to encompass operational continuity in the event of blockchain system disruptions,⁴³ cyberattacks,⁴⁴ or digital infrastructure failures.⁴⁵ This approach is consistent with findings from various studies that identify technological vulnerabilities as a primary source of risk within the ecosystem.⁴⁶

The third characteristic indicates that POJK No. 27 of 2024 employs a layered legal protection model. This can be seen in the rule requiring the use of hot storage, cold storage, multi-signature wallets, and smart contract wallets simultaneously. The goal of

⁴¹ Tosato, Dick, and Odinet.

⁴² T Zauha, 'Unpredictability and Consequence in Play-to-Earn Crypto Gaming', *Information Communication and Society*, 28.7 (2025), pp. 1233–51, doi:10.1080/1369118X.2024.2326654.

⁴³ Rainer Alt and Max Gräser, 'Distributed Ledger Technology', *Electronic Markets*, 35.1 (2025), p. 53, doi:10.1007/s12525-025-00784-w.

⁴⁴ Udit Agarwal and others, 'Blockchain and Crypto Forensics: Investigating Crypto Frauds', *International Journal of Network Management*, 34.2 (2024), doi:10.1002/nem.2255.

⁴⁵ F G Taştan, 'Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA', *European Review of Private Law*, 33.5–6 (2025), pp. 1125–44, doi:10.54648/erpl2025069.

⁴⁶ Sidik and others.

this model is to reduce the risks of digital asset theft, crypto wallet hacking, and unauthorized access. These protective steps show that the regulation aims to turn blockchain-related technology risks into clear legal duties.⁴⁷

The fourth characteristic indicates the existence of a preventive legal protection model against the risks of money laundering and blockchain anonymity. The POJK requires systems to prevent the receipt or transfer of assets from unclear sources, prevent transaction mixing practices, and implement authorization mechanisms for parties conducting transactions. This characteristic demonstrates that investor protection is not only aimed at individual losses but also at systemic risks arising from the use of blockchain by financial criminals.

The Decree of POJK No. 27 of 2024 establishes a legal protection model grounded in transparency and traceability, referred to as the traceability protection model.⁴⁸ Mandates such as assigning unique identifiers to each transaction, recording transactions in real time, maintaining comprehensive transaction records, and retaining data for up to ten years collectively create a robust evidentiary framework.⁴⁹ This framework facilitates dispute resolution, addresses asset misuse, and supports investigations of legal violations. By ensuring the availability of digital evidence, the framework enhances the enforcement of investors' rights.⁵⁰

In the context of further implementing a legal protection model based on independent oversight, termed independent audit protection. Storage systems and facilities are required to undergo audits conducted by independent institutions with expertise in information systems.⁵¹ Audit outcomes create obligations to repair or replace systems that do not meet established standards. This framework indicates that investor protection is reinforced not only through voluntary compliance by business entities but also through external verification mechanisms that serve as preventive legal controls.⁵²

Meanwhile, the decree POJK No. 27 of 2024 exemplifies a preventive model of technological legal protection. Unlike repressive models that address disputes only after losses occur, POJK emphasizes prevention through information security standards, risk mitigation strategies, system audits, transaction controls, and the safeguarding of digital

⁴⁷ A D Popescu and C M Spulbar, *Financial Digital Assets and the Financial Risk Modeling of Portfolio Investments*, *Financial Digital Assets and the Financial Risk Modeling of Portfolio Investments*, 2025, doi:10.4018/979-8-3693-8120-5.

⁴⁸ 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*, 4.8 (2025), doi:10.55324/josr.v4i8.2726.

⁴⁹ D Liebau, 'Introduction to Centralized Finance', *The Blockchain Scholars Book: Current Academic Insights Condensed for Busy Practitioners*, 2025, pp. 35–40, doi:10.1007/978-981-95-2844-8_7.

⁵⁰ Irawan and Christianto.

⁵¹ A Sumera and B.V.R.V. Tej, 'Impact of Token Economics on AMM Efficiency', *Studies in Systems, Decision and Control*, 2025, 223–34, doi:10.1007/978-3-031-96641-5_20.

⁵² S Ioannou and others, 'Exploring the Landscape of Tokenization: A Comprehensive Systematic Literature Review', *Handbook of Blockchain Technology*, 2025, pp. 108–26, doi:10.4337/9781803922805.00017.

assets.⁵³ The principal normative finding of this study is that POJK No. 27 of 2024 establishes an investor protection regime centred on blockchain risk prevention by utilizing technological security measures, transaction traceability, and standardized governance of digital asset custody.⁵⁴

3.3 Towards Legal Protection in Blockchain Risk

This discussion frames legal protection for cryptocurrency investors as a normative instrument designed to ensure the sustainability of legal relationships among investors, cryptocurrency service providers, and regulators.⁵⁵ Legal protection refers to the ability of interested parties to enforce the rights granted to them effectively. Meanwhile, Barros views legal protection as a set of rules that safeguards individuals' interests and rights from the actions of others.⁵⁶

If these two perspectives are synthesized with the evolution of the blockchain ecosystem, legal protections for crypto investors are intended not only to shield them from potentially harmful regulatory actions but also from risks posed by platform operators, blockchain protocol developers, cybercriminals, and other market actors. Thus, the main issue in the crypto industry is not merely the legality of digital assets, but rather how the legal system can ensure the effective protection of investor rights in a decentralized technological environment.⁵⁷

The necessity for legal protection is heightened by its role in maintaining stable legal relationships and preventing violations.⁵⁸ Recent literature indicates that blockchain technology introduces novel forms of risk not present in conventional financial systems. Didenko explains that the characteristics of tokens, tokenization, and the diverse rights associated with crypto assets generate a broad spectrum of legal risks. This complexity renders the legal relationship between investors and digital assets increasingly challenging to delineate.⁵⁹

In this context, legal protection should not be viewed solely as a dispute-resolution mechanism following a loss. Instead, it functions as an instrument that maintains the stability of legal relationships from the outset of an investor's engagement with the blockchain ecosystem.⁶⁰

⁵³ S Li, 'FROM CONTAGION TO CONTAINMENT: A REVIEW OF SYSTEMIC FINANCIAL RISK AND REGULATORY GOVERNANCE', *Journal of Governance and Regulation*, 14.4 Special Issue (2025), pp. 342–57, doi:10.22495/jgrv14i4siart11.

⁵⁴ Carvalho.

⁵⁵ Didenko.

⁵⁶ Marcos Barros and Ghazal Zulfiqar, 'Critical Methodologies: Opening up Space to Unpack Power and Explore Critical Alternatives in Conducting and Writing Research', *Organization*, 32.6 (2025), pp. 781–89, doi:10.1177/13505084251372994.

⁵⁷ Abdulrazak Alenazi and others, 'Cleanliness Is next to Godliness: Can Money Laundering Be Sharia-Compliant?', *Journal of Financial Crime*, May, 2024, pp. 584–94, doi:10.1108/JFC-05-2024-0169.

⁵⁸ Elana Shohamy, 'Critical Language Testing, Multilingualism and Social Justice', *TESOL Quarterly*, 56.4 (2022), pp. 1445–57, doi:10.1002/tesq.3185.

⁵⁹ Didenko.

⁶⁰ Pocher, 'Crypto-Asset Ecosystems and the EU Anti-Money Laundering Framework: Law and Technology Perspectives'.

Legal protection requires clear norms, procedures, and mechanisms to govern the parties' rights and obligations. Jaffri's literature on crypto asset regulation in the United States indicates that a regulatory approach overly reliant on enforcement (enforcement-based regulation) leads to legal uncertainty and uneven investor protection.⁶¹ These findings demonstrate that without systematic norms, investors struggle to understand the legal status of assets, the responsibilities of operators, and the available protection mechanisms in the event of losses.⁶²

The dimension of legal protection is also closely linked to the existence of rules governing the legal relationship between investors and cryptocurrency service providers.⁶³ Legal protection can stem from legislation or agreements. In the context of blockchain, these two sources of protection coexist.⁶⁴ On the one hand, there are government regulations governing cryptocurrency trading activities. On the other hand, there are electronic agreements, such as terms of service, smart contracts, and other digital clauses, that bind platform users. Therefore, the effectiveness of investor legal protection depends heavily on the legal system's ability to integrate external protection provided by regulations with internal protection provided by digital contracts.⁶⁵

Lising's study on infrastructure tokenization and the case of Axie Infinity in the Philippines shows that social risks in blockchain technology are not only related to technological security aspects, but also to the issue of inequality in the distribution of economic benefits. The findings show that people with low levels of financial literacy tend to be more vulnerable to losses than groups with stronger economic capital. When viewed through the theory of legal protection, this phenomenon confirms that the existence of legal norms alone is not enough to ensure the protection of investors' rights. Legal protection needs to include substantive aspects so that investor rights can be effectively exercised, without being hampered by information gaps, low digital literacy, and economic inequality.

Hadjon emphasizes that preventive legal protection aims to prevent legal violations and minimize the occurrence of disputes.⁶⁶ In the cryptocurrency industry, preventive protection can be achieved through information transparency requirements, risk disclosure, system security audits, user identity verification, and investor education.⁶⁷ These instruments serve to prevent losses before they occur. In other words, investor protection should be measured not only by the availability of compensation mechanisms after losses occur, but also by the ability of regulations to reduce the probability of losses from the outset.⁶⁸

Carvalho's literature on cryptocurrency custody further underscores the importance of preventive legal protections. Carvalho points out that investors face a dilemma

⁶¹ D Kochergin, 'CRYPTO-ASSETS: ECONOMIC NATURE, CLASSIFICATION AND REGULATION OF TURNOVER', *International Organisations Research Journal*, 17.3 (2022), doi:10.17323/1996-7845-2022-03-04.

⁶² Ledoux and Smaili.

⁶³ Belikoff and Blazsek.

⁶⁴ D A Zetsche, 'Third-Country Multi-Issuer Stablecoins', *ERA Forum*, 2025, doi:10.1007/s12027-025-00866-4.

⁶⁵ de Souza, Lima, and Almeida.

⁶⁶ Philipus M Hadjon, *Fungsi Normatif Hukum Administrasi Dalam Mewujudkan Pemerintahan Yang Bersih* / Philipus M. Hadjon, 1994, MCMXCIV.

⁶⁷ Hadjon, MCMXCIV.

⁶⁸ Hadjon, MCMXCIV.

between self-custody and third-party custody. Self-custody gives investors full control but carries the risk of asset loss due to user error.⁶⁹ Conversely, third-party custody offers operational convenience and security, but presents the risk of custodian failure. These findings suggest that investor legal protection should focus on risk management before losses occur, for example, through proof-of-reserves requirements, independent audits, operational risk management, and security standards for digital asset storage.⁷⁰

Preventive legal protection can also be found in the utilization of technology to monitor blockchain transactions. Dhore and his colleagues' research on *the Crypto-Monitoring Tool* shows that the use of blockchain chart analysis and transaction mapping can help identify high-risk digital wallets as well as detect activities that lead to fraud.⁷¹ When viewed from the theory of legal protection, the technology can be understood as a means of prevention that provides an opportunity for regulators and service providers to reduce risks from the initial stage. In this context, legal protection is not only present in the form of written norms, but is also realized through a technology-based supervision system.

In addition to preventive protection, Hadjon also explained the importance of repressive legal protection as a mechanism for resolving disputes.⁷² This protection is applied after investors have suffered losses, especially if prevention efforts have not succeeded in avoiding investors from risks. In the blockchain ecosystem, repressive protection can be realized through the filing of objections, compensation demands, asset recovery, and legal action against the party who committed the violation.⁷³ Therefore, administrative, civil, and criminal sanctions are an inseparable element of repressive legal protection, because they play a role in restoring investors' rights and providing a preventive effect against similar violations.⁷⁴

The need for law enforcement measures is increasingly evident in Dulisse and his colleagues' research on cryptocurrency-based money laundering in Southeast Asia. The study shows that cryptocurrencies have been used as an important financial infrastructure in transnational crimes, including fraud networks and money laundering practices. This condition shows that the prevention mechanism is not always able to anticipate all forms of abuse of blockchain technology. Therefore, repressive legal protection is needed to take action against perpetrators, provide compensation to victims, and maintain the integrity of the digital asset market.

However, legal protection theory suggests that the effectiveness of protection is not determined solely by the existence of preventive and repressive norms. In the context of crypto assets, practical legal protection can be measured by regulators', judicial institutions', and law enforcement agencies' ability to handle disputes involving

⁶⁹ Carvalho.

⁷⁰ Ali and Vidan.

⁷¹ Dhore and others.

⁷² Hadjon, MCMXCIV.

⁷³ L Stern, 'Regulating Cryptocurrencies in a Post-Pandemic Global Economy: A Comparative Legal Analysis of the EU, the US, and Russia', *Journal of Economic Criminology*, 9 (2025), doi:10.1016/j.jeconc.2025.100183.

⁷⁴ J Buchan and M Üngör, 'Monetary Sovereignty in the Digital Age: The Role of Central Bank Digital Currencies', *International Journal of Political Economy*, 55.1 (2026), pp. 88–108, doi:10.1080/08911916.2026.2624900.

blockchain technology. Without adequate institutional capacity, legal protection norms will merely become formal rules that are difficult to implement effectively.⁷⁵

The issue of practical legal protection is becoming increasingly important because blockchain is inherently cross-jurisdictional. Jaffri points out that one of the main challenges in crypto regulation is cross-border oversight and regulatory arbitrage. Investors can trade through platforms operating in various countries with different legal regimes. This situation makes enforcing investor rights far more complex than in conventional financial transactions. Therefore, practical legal protection requires coordination among authorities, international cooperation, and effective cross-jurisdictional oversight mechanisms.⁷⁶

From the perspective of legal protection, safeguarding the rights and interests of legal entities, crypto investors are, in essence, legal entities entitled to guarantees of security, transparency, and legal certainty. Meanwhile, crypto asset service providers are obligated to provide a secure, transparent, and accountable system. It is this relationship between investor rights and provider obligations that lies at the heart of legal protection in the blockchain industry. When one of these elements is not functioning proportionally, the risk of investor loss increases. A synthesis of the entire literature indicates that the primary risks associated with blockchain are no longer limited to the price volatility of digital assets. These risks have evolved into multidimensional risks encompassing cybersecurity, custodial failures, money laundering, social inequality, governance weaknesses, and regulatory uncertainty. Therefore, investor legal protection must be comprehensively designed by integrating legal, practical, preventive, and repressive legal protections into a single, mutually complementary framework.⁷⁷

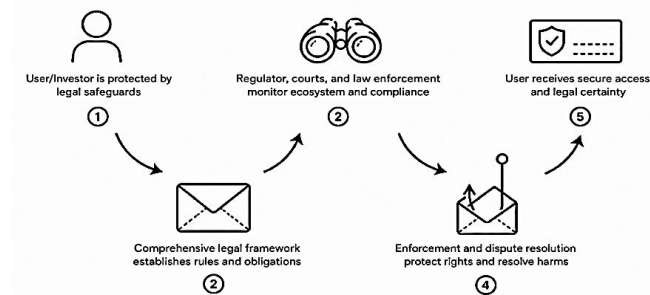


Fig. 2. Legal Protection Model and Blockchain Risk

⁷⁵ Hadjon, MCMXCIV.

⁷⁶ D Kamensky and others, 'Corporate Compliance Programs in the Global Environment: Business, "Binance" and Beyond', *Studies in Systems, Decision and Control*, 2025, 927–37, doi:10.1007/978-3-031-71526-6_83.

⁷⁷ V Comegna, 'The Persistence of the Opposites: Ai and Blockchain for Transparent and Secure Cross-Regulatory Compliance and Enforcement Cooperation Test Beds in the Eu Digital Acquis', *Journal of Law, Market and Innovation*, 4.2 (2025), pp. 327–57, doi:10.13135/2785-7867/12273.

Based on an analysis of legal protection theory and a synthesis of prior research, the most relevant legal protection model for the blockchain ecosystem is the integrative model. This model positions legal protection as the normative foundation, preventive legal protection as a risk mitigation tool, repressive legal protection as a mechanism for restoring investors' rights, and practical legal protection as a means of implementation through effective law enforcement. With this approach, legal protection not only serves to resolve disputes after losses have occurred, but also maintains investor legal relationships in a fair, safe, and sustainable condition, in accordance with the objectives of legal protection formulated by Semyonovkyh.

3.4 Discussion

This discussion frames legal protection for cryptocurrency investors as a normative instrument designed to ensure the sustainability of legal relationships among investors, cryptocurrency service providers, and regulators. Legal protection refers to the ability of interested parties to enforce the rights granted to them effectively.⁷⁸ Meanwhile, Barros views legal protection as a set of rules that safeguards individuals' interests and rights from the actions of others.⁷⁹ This discussion examines legal protections for cryptocurrency investors to maintain stable legal relationships among investors, service providers, and regulators. The issue of practical legal protection is becoming increasingly important because blockchain is inherently cross-jurisdictional. Jaffri points out that one of the main challenges in crypto regulation is cross-border oversight and regulatory arbitrage. Investors can trade through platforms operating in various countries with different legal regimes.

This situation makes the enforcement of investor rights far more complex than in conventional financial transactions. Therefore, practical legal protection requires coordination among authorities, international cooperation, and effective cross-jurisdictional oversight mechanisms. From the perspective of legal protection as safeguarding the rights and interests of legal entities, crypto investors are, in essence, legal entities entitled to guarantees of security, transparency, and legal certainty. Meanwhile, crypto asset service providers are obligated to provide a secure, transparent, and accountable system. It is this relationship between investor rights and provider obligations that lies at the heart of legal protection in the blockchain industry. When one of these elements is not functioning proportionally, the risk of investor loss increases.⁸⁰ A synthesis of the entire literature indicates that the primary risks associated with blockchain are no longer limited to the price volatility of digital assets. These risks have evolved into multidimensional risks encompassing cybersecurity, custodial failures, money laundering, social inequality, governance weaknesses, and regulatory uncertainty.

The findings from the literature indicate that the storage and management of digital financial assets, which involve risks such as technological risks, cyber risks, asset theft, transaction abuse, and system failures, must employ protective mechanisms

⁷⁸ Hadjon, MCMXCIV.

⁷⁹ Barros and Zulfikar.

⁸⁰ Babenko and others.

that are preventive, multi-layered, measurable, auditable, transparent, and traceable. POJK No. 27 of 2024 has essentially incorporated these principles through system security, risk mitigation, asset storage management, transaction controls, business continuity, traceability, and independent audits. However, when considered in light of the scope of POJK No. 27 of 2024, the available protections remain more focused on institutional risks than on the dynamically emerging risks inherent to blockchain characteristics. This gap is evident in risks related to DeFi, smart contracts, tokenomics, regulatory arbitrage, decentralized governance, wallet fraud, algorithm-based market manipulation, custody risk, and cross-jurisdictional blockchain mechanisms. This means that the scope of protection under POJK No. 27 of 2024 has not yet fully kept pace with the transformation of blockchain risk objects. The nature of the risks identified extends beyond the relationship between investors and institutions directly supervised by Indonesian authorities.⁸¹

The blockchain ecosystem also involves developers, validators, DAOs, smart contracts, liquidity providers, decentralized exchanges, wallet providers, and protocols that can operate without an easily identifiable legal entity structure. This is because the nature of blockchain allows economic activities to take place beyond geographical boundaries and conventional national institutional structures. Blockchain technology architecture is highly decentralized, whereas POJK No. 27 of 2024 is based on the identification of legal entities; meanwhile, some blockchain risks actually arise from mechanisms that do not always have a single party that can be directly held accountable. Smart contracts can execute transactions automatically, DAOs can distribute decision-making, validators perform network functions, while developers or protocol developers may be located in different jurisdictions.⁸²

As a result, the principle that every risk must be convertible into a legal liability faces the issue of a legal accountability gap. The existence of gaps in socioeconomic inequality, regulatory arbitrage, wallet fraud, mixing services, custody loss, misleading DeFi intermediaries, the decentralization defense, Ponzi-like tokenomics, governance failure, and algorithmic market manipulation demonstrates that blockchain risks are not merely system security risks, but also encompass governance risks, benefit distribution risks, market behavior risks, and legal accountability risks. This means that the primary premise of preventive protection is not merely to secure systems managed by operators, but must also be capable of anticipating risks arising from protocols, code, decentralized governance, token structures, and cross-jurisdictional relationships.⁸³

The crypto investor transaction ecosystem not only interacts with centralized digital asset platforms but also extends into the DeFi ecosystem, smart contracts, asset tokenization, blockchain gaming, staking, decentralized governance, and cross-jurisdictional transactions, as confirmed by Lising's (2026) research. The crypto ecosystem reveals disparities in benefits and risks regarding infrastructure tokenization and Axie Infinity (Jaffri, 2026), indicating issues of legal uncertainty and regulatory arbitrage (M. Dhore et al., 2026), which demonstrate the use of blockchain forensics to detect high-risk wallets; Dulisse et al. (2026) demonstrate the growing use of cryptocurrency in organized fraud networks; while Carvalho (2026) highlights custody

⁸¹ Lising.

⁸² Dhore and others.

⁸³ Dulisse, Denis, and Connealy.

risks and low transparency within the DeFi ecosystem.⁸⁴ Findings by Kokorin (2025) on “decentralization defense,” De Souza et al. (2025) and Ali & Vidan (2025) on Ponzi-like tokenomics, Ledoux and Smaili (2025) on governance failure, and Lee and Schu (2025) on blockchain-based market abuse increasingly indicate that these risks are not a fleeting phenomenon.⁸⁵ This means that the research findings have medium- and long-term relevance, particularly if the development of blockchain technology outpaces the regulatory capacity to identify and control new forms of risk.⁸⁶

The investor protection model in POJK No. 27 of 2024 needs to evolve from institutional preventive protection to adaptive blockchain-risk preventive protection. This concept expands the obligations of operators to conduct blockchain risk assessments, disclose risks related to smart contracts and DeFi, perform tokenomics analysis prior to marketing, utilize blockchain analytics to detect risky transaction patterns, implement protection mechanisms against loss of cryptographic access, provide proof of reserves, conduct real-time or periodic blockchain audits, and establish accountability mechanisms when losses stem from decentralized protocols or cross-jurisdictional actors. The theoretical contribution of this research lies in the expansion of the concept of preventive legal protection: protection no longer means merely preventing institutional failure, but also preventing and anticipating risks inherent in the blockchain architecture itself. However, the study’s limitations should be noted, as this analysis is primarily normative-doctrinal in nature and relies on literature reviews to identify gaps between legal norms and evolving risks; this study has not yet empirically measured the frequency of investor losses or the effectiveness of each POJK instrument.⁸⁷

Therefore, future research could develop empirical testing through case studies, analysis of blockchain transaction data, cross-jurisdictional regulatory comparisons, and risk mapping between types of blockchain risks and legal protection mechanisms. Given that the evolution of blockchain risks has surpassed the institutional risks explicitly anticipated by POJK No. 27 of 2024 and now encompasses DeFi, smart contracts, tokenomics, custody, regulatory arbitrage, decentralization, market manipulation, and cross-jurisdictional risks, POJK No. 27 of 2024 needs to be expanded into an adaptive legal protection model based on blockchain risks so that the principles of prevention, layering, measurability, auditability, and transparency remain effective against dynamically evolving forms of blockchain risk.⁸⁸

4 Conclusion

This study concludes that the legal protection framework for crypto investors in POJK No. 27 of 2024 has essentially adopted an integrative legal protection model through regulations governing the rights and obligations of the parties, operator governance, risk management, supervision, and compliance enforcement mechanisms. From a legal protection theory perspective, these regulations represent legal protection as a

⁸⁴ Dhore and others.

⁸⁵ Lee and Schu.

⁸⁶ Dulisse, Denis, and Connealy.

⁸⁷ Dulisse, Denis, and Connealy.

⁸⁸ Dulisse, Denis, and Connealy.

normative foundation, preventive legal protection through risk mitigation and governance obligations, and repressive legal protection through sanction mechanisms and the resolution of violations. However, this study finds that the multidimensional risks of blockchain, such as cybersecurity risks, custodial failures, money laundering, cross-jurisdictional regulatory arbitrage, and technological uncertainty, require strengthening practical legal protections so that established norms can be effectively implemented. Theoretically, this research contributes to the development of a conceptual framework in the form of an Integrative Legal Protection Model for the Blockchain Ecosystem. The model combines preventive, repressive, and practical legal protection aspects in a single framework geared toward providing more comprehensive protection for cryptocurrency investors. In practical terms, the results of this study provide recommendations to regulators to strengthen supervisory capacity, improve inter-agency coordination, expand international cooperation, and build risk-based law enforcement mechanisms in the blockchain ecosystem. The limitations of this research lie in the scope of its study, which still focuses on normative analysis of POJK No. 27 of 2024 and literature review. Therefore, this study has not directly tested the effectiveness of the implementation of these regulations in practice. Thus, further research needs to be directed at empirical studies on the effectiveness of crypto investor protection, institutional capacity in law enforcement, cross-jurisdictional dispute resolution mechanisms, and the integration of cybersecurity and blockchain governance approaches into the crypto asset legal protection system in Indonesia.

REFERENCES

- Agarwal, Udit, Vinay Rishiwal, Sudeep Tanwar, and Mano Yadav, 'Blockchain and Crypto Forensics: Investigating Crypto Frauds', *International Journal of Network Management*, 34.2 (2024), doi:10.1002/nem.2255
- Agustina, Refi, and Fita Nurotul Faizah, 'Sharia Fintech: Opportunities and Challenges in Indonesia', *Journal of Islamic Economics (JoIE)*, 3.1 (2023), pp. 61–75, doi:10.21154/joie.v3i1.6289
- Alenazi, Abdulrazak, Abdelaziz Chazi, Eid M Alotaibi, and Kimberly Gleason, 'Cleanliness Is next to Godliness: Can Money Laundering Be Sharia-Compliant?', *Journal of Financial Crime*, May, 2024, pp. 584–94, doi:10.1108/JFC-05-2024-0169
- Ali, J, and G Vidan, 'Playing, Earning, Crashing, and Grinding: Axie Infinity and Growth Crises in the Web3 Economy', *Big Data and Society*, 12.3 (2025), doi:10.1177/20539517251357296
- Alt, Rainer, and Max Gräser, 'Distributed Ledger Technology', *Electronic Markets*, 35.1 (2025), p. 53, doi:10.1007/s12525-025-00784-w
- Babenko, T, K Kolesnikova, M Panchenko, O Abramkina, N Kiktev, Y Meish, and others, 'Risk Assessment of Cryptojacking Attacks on Endpoint Systems: Threats to Sustainable Digital Agriculture', *Sustainability (Switzerland)*, 17.12 (2025), doi:10.3390/su17125426
- Barros, Marcos, and Ghazal Zulfikar, 'Critical Methodologies: Opening up Space to Unpack Power and Explore Critical Alternatives in Conducting and Writing Research', *Organization*, 32.6 (2025), pp. 781–89, doi:10.1177/13505084251372994
- Belikoff, V, and V Blazsek, 'A Systematisation of Legal-Regulatory Risks Related to Central Bank Digital Currencies: A Comparative Analysis of the US, the UK and China', *Law and Financial Markets Review*, 18.2 (2025), pp. 73–101, doi:10.1080/17521440.2025.2526326
- Bijleveld, Catrien, 'Methods for Empirical Legal Research', in *Digital Decade* (Nomos Verlagsgesellschaft mbH & Co. KG, 2025), pp. 21–40, doi:10.5771/9783748943990-21
- Buchan, J, and M Üngör, 'Monetary Sovereignty in the Digital Age: The Role of Central Bank Digital Currencies', *International Journal of Political Economy*, 55.1 (2026), pp. 88–108, doi:10.1080/08911916.2026.2624900
- Cao, Y, M Dai, S Kou, L Li, and C Yang, 'Designing Stablecoins', *Mathematical Finance*, 35.1 (2025), pp. 263–94, doi:10.1111/mafi.12445
- Carvalho, A, 'Cryptocurrency Custody', *Elgar Encyclopedia of Cryptocurrencies, Blockchain and DLT*, 2026, pp. 52–55, doi:10.4337/9781035339969.00016
- Chen, Xiaoting Xiaoyu Xian Xun, Min Yeh Tsai, Peter G. Wolynes, Gabriela da Rosa, Leandro Grille, Victoria Calzada, and others, 'No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title', *Nucleic Acids Research*, 6.1 (2018), pp. 1–7
<http://dx.doi.org/10.1016/j.gde.2016.09.008>
<http://dx.doi.org/10.1007/s00412-015-0543-8>
<http://dx.doi.org/10.1038/nature08473>
<http://dx.doi.org/10.1016/j.jmb.2009.01.007>
<http://dx.doi.org/10.1016/j.jmb.2012.10.008>
<http://dx.doi.org/10.1038/s4159>

- Comegna, V, 'The Persistence of the Opposites: Ai and Blockchain for Transparent and Secure Cross-Regulatory Compliance and Enforcement Cooperation Test Beds in the Eu Digital Acquis', *Journal of Law, Market and Innovation*, 4.2 (2025), pp. 327–57, doi:10.13135/2785-7867/12273
- Dhore, M, S M Jaybhave, A Vimal, A Agrawal, R Bajaj, and R Barde, 'Crypto-Monitoring Tool', *Studies in Systems, Decision and Control*, 2026, 863–73, doi:10.1007/978-3-031-85398-2_76
- Didenko, A, 'Blockchain and Crypto-Assets', *Handbook of Blockchain in Public Governance*, 2026, pp. 219–31, doi:10.4337/9781035330096.00028
- Dulisse, B C, J Denis, and N Connealy, 'Exploring the Extent of International Money Laundering Using Cryptocurrency: A Systematic Scoping Review of Gaps in Research on Southeast Asia's Scam Economy', *Journal of Money Laundering Control*, 2026, pp. 1–19, doi:10.1108/JMLC-12-2025-0241
- Gong, Y, K P Chow, and S M Yiu, 'Improved Bitcoin Simulation Model and Address Heuristic Method', *Forensic Science International: Digital Investigation*, 53 (2025), doi:10.1016/j.fsidi.2025.301935
- Hadjon, Philipus M, *Fungsi Normatif Hukum Administrasi Dalam Mewujudkan Pemerintahan Yang Bersih / Philipus M. Hadjon*, 1994, MCMXCIV
- Iefymenko, T I, and T L Dmytrenko, 'DEVELOPMENT AND INTEGRATION OF DIGITAL CURRENCIES IN THE VIRTUAL ASSET MARKET', *Science and Innovation*, 21.2 (2025), pp. 3–14, doi:10.15407/scine21.02.003
- Ioannou, S, S Louca, C Savvides, and E Iosif, 'Exploring the Landscape of Tokenization: A Comprehensive Systematic Literature Review', *Handbook of Blockchain Technology*, 2025, pp. 108–26, doi:10.4337/9781803922805.00017
- 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*, 4.8 (2025), doi:10.55324/josr.v4i8.2726
- 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)*, 2024, pp. 2465–77, doi:10.23917/iseth.5163
- Jaffri, A M, 'Regulating Crypto Assets in the United States: Balancing Regulatory Effectiveness, Investor Protection, and Cross-Border Challenges', *Capital Markets Law Journal*, 21.2 (2026), doi:10.1093/cmlj/kmag015
- Kamensky, D, Y Danylevska, V Hrankina, A Koriahina, and A Udod, 'Corporate Compliance Programs in the Global Environment: Business, "Binance" and Beyond', *Studies in Systems, Decision and Control*, 2025, 927–37, doi:10.1007/978-3-031-71526-6_83
- Karminsky, A, and M Stolbov, *Systemic Financial Risk: An Emerging Market Perspective*, *Systemic Financial Risk: An Emerging Market Perspective*, 2024, doi:10.1007/978-3-031-54809-3
- Kochergin, D, 'CRYPTO-ASSETS: ECONOMIC NATURE, CLASSIFICATION AND REGULATION OF TURNOVER', *International Organisations Research Journal*, 17.3 (2022), doi:10.17323/1996-7845-2022-03-04
- Kokorin, I, 'The Decentralisation Defence', *Computer Law and Security Review*, 57 (2025), doi:10.1016/j.clsr.2025.106148

- Ledoux, E L, and N Smaili, 'Cryptocurrency Frauds: The FTX Story', *Journal of Financial Crime*, 32.3 (2025), pp. 530–44, doi:10.1108/JFC-01-2024-0022
- Lee, J, and L Schu, 'Market Abuse in the Cryptoassets Market: Same Risks, Same Activities, and Same Regulatory Outcomes?', *A Research Agenda for Financial Law and Regulation*, 2025, pp. 157–78, doi:10.4337/9781803929996.00015
- Li, S, 'FROM CONTAGION TO CONTAINMENT: A REVIEW OF SYSTEMIC FINANCIAL RISK AND REGULATORY GOVERNANCE', *Journal of Governance and Regulation*, 14.4 Special Issue (2025), pp. 342–57, doi:10.22495/jgrv14i4siart11
- Liebau, D, 'Introduction to Centralized Finance', *The Blockchain Scholars Book: Current Academic Insights Condensed for Busy Practitioners*, 2025, pp. 35–40, doi:10.1007/978-981-95-2844-8_7
- Lising, P J L, 'Reassessing Blockchain in Global Development: Tokenization of Infrastructure, Social Impacts, and the Axie Infinity Case in the Philippines', *Social Sciences and Humanities Open*, 13 (2026), doi:10.1016/j.ssaho.2025.102340
- McNab, H., and A. Wynn, *Principles and Practice of Consumer Credit Risk Management*, CIB Publishing, 2000
- Oranburg, S C, 'Function Over Form: Toward a Safe Harbor Framework for DeFi Regulation of Utility Tokens', *Louisiana Law Review*, 86.1 (2025), pp. 81–166
- Otoritas Jasa Keuangan, R.I, *POJK Nomor 27 Tahun 2024* (2024)
- Perdana, A, S V Bharathi, R Karim, S Arifin, and A Srivastava, *Digital Strategy and Governance in Transformative Technologies*, *Digital Strategy and Governance in Transformative Technologies*, 2025, doi:10.1201/9781003477808
- Pocher, N, 'Crypto-Asset Ecosystems and the EU Anti-Money Laundering Framework: Law and Technology Perspectives', *Law, Governance and Technology Series*, 2025, 1–297, doi:10.1007/978-3-031-94698-1
- , 'Traceability of Crypto-Asset Transfers under the New EU AML/ CFT Regime: The Crypto Travel Rule between Challenges and Open Issues', *A Research Agenda for Financial Law and Regulation*, 2025, pp. 197–219, doi:10.4337/9781803929996.00017
- Popescu, A D, and C M Spulbar, *Financial Digital Assets and the Financial Risk Modeling of Portfolio Investments*, *Financial Digital Assets and the Financial Risk Modeling of Portfolio Investments*, 2025, doi:10.4018/979-8-3693-8120-5
- Rambe, Tamiarisa Amanda Fasa, Sunarmi Sunarmi, Mahmud Siregar, and Detania Sukarja, 'Kewenangan Badan Penyelesaian Sengketa Konsumen Kota Medan Memeriksa Sengketa Konsumen Jasa Keuangan Pasca Terbentuknya Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan', *Locus Journal of Academic Literature Review*, 1.2 (2022), pp. 109–16, doi:10.56128/ljoalr.v1i2.57
- Shapiro, S P, 'Crypto Fever: Law, Regulation, and the Promise of Trustless Trust', *Annual Review of Law and Social Science*, 21.1 (2025), pp. 87–105, doi:10.1146/annurev-lawsocsci-110124-063008
- Shohamy, Elana, 'Critical Language Testing, Multilingualism and Social Justice', *TESOL Quarterly*, 56.4 (2022), pp. 1445–57, doi:10.1002/tesq.3185
- 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*, 23.1 (2025), pp. 229–64, doi:10.28918/jhi.v23i1.08

- de Souza, P V S, R S Lima, and R B Almeida, 'Red Flags in Play-to-Earn Crypto Games: Proposal and Testing of a Checklist Based on Ponzi Scheme', *Revista de Contabilidade e Organizacoes*, 19 (2025), doi:10.11606/issn.1982-6486.rco.2025.230807
- Stern, L, 'Regulating Cryptocurrencies in a Post-Pandemic Global Economy: A Comparative Legal Analysis of the EU, the US, and Russia', *Journal of Economic Criminology*, 9 (2025), doi:10.1016/j.jeconc.2025.100183
- Sumera, A, and B.V.R.V. Tej, 'Impact of Token Economics on AMM Efficiency', *Studies in Systems, Decision and Control*, 2025, 223–34, doi:10.1007/978-3-031-96641-5_20
- Taştan, F G, 'Strict Liability of Crypto-Asset Service Providers: Turkish Law's Sui Generis Response to MICA', *European Review of Private Law*, 33.5–6 (2025), pp. 1125–44, doi:10.54648/erpl2025069
- Tosato, A, D L Dick, and C K Odinet, 'DEBT TOKENS', *University of Pennsylvania Law Review*, 173.4 (2025), pp. 1103–71, doi:10.58112/uplr.173-4.3
- Wilson, Paulina E., 'Comparative Law in Legal Education: An Interdisciplinary Perspective', *Juridical Tribune - Review of Comparative and International Law*, 14.3 (2024), pp. 345–62, doi:10.62768/TBJ/2024/14/3/01
- Wirananda, Henny Andriyani, Wan Dian Safina, and Wilda Sri Munawaroh Harahap, 'The Role of Internal Control Over Sales, Receivables, Cash Receipts, and Cash Disbursements At Pt. Indako Trading Co', *Strategic Management Business Journal*, 2.02 (2022), pp. 99–104, doi:10.55751/smbj.v2i02.52
- Zauch, T, 'Unpredictability and Consequence in Play-to-Earn Crypto Gaming', *Information Communication and Society*, 28.7 (2025), pp. 1233–51, doi:10.1080/1369118X.2024.2326654
- Zeiß, C, L Straub, M Greiner, M Neis, N Neis, A Winkelmann, and others, 'Exploring Trust in Decentralized Finance Intermediaries: A Taxonomy and Archetypes for Guiding Blockchain-Based Investment Decisions on the Web', *Internet Research*, 35.7 (2025), pp. 133–52, doi:10.1108/INTR-01-2025-0156
- Zetzsche, D A, 'Third-Country Multi-Issuer Stablecoins', *ERA Forum*, 2025, doi:10.1007/s12027-025-00866-4