

Article

Criminal Liability for Crypto Asset Investment Crime from the Perspective of Cyber Economic Criminal Law in Indonesia

Abdoel Muthalib Marassabessy

¹Master of Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article information	Abstract
DOI : xxx Correspondence :	The development of digital technology and blockchain systems has driven increased crypto-asset investment activity in Indonesia, but it has also given rise to various forms of cyber-based investment crime that harm society at large. Crypto-asset investment crimes—including fraud, Ponzi schemes, digital-platform manipulation, and illegal investment operations—have complex characteristics because they are committed in cyberspace, cross jurisdictional boundaries, and involve digital financial instruments that the public does not yet fully understand. This situation raises legal issues concerning the concept and regulation of criminal liability for perpetrators within the framework of cyber-economic criminal law. This study analyses the concept of criminal liability for crypto-asset investment crime and examines its treatment under Indonesian legislation. It uses a normative juridical method with statutory and conceptual approaches. The results show that liability may be imposed on both individuals and corporations on the basis of fault, but existing rules remain sectoral and have not been comprehensively integrated into the cyber-economic criminal-law system. Regulatory harmonisation and reform are therefore required to strengthen legal certainty, effective enforcement, and legal protection for crypto-asset investors in Indonesia.
Submission Track	
Submission : April 18, 2026 Final Review : May 20, 2026 Accepted : May 25, 2026	
Keywords	
crypto-asset investment, cybercrime, criminal liability, economic criminal law, legal certainty	
 This is an open access article under the CC BY https://creativecommons.org/licenses/by/4.0/	

INTRODUCTION

Developments in information and communication technology have brought significant transformation to the economic sector, including the emergence of crypto-assets as digital investment instruments based on blockchain technology (Manullang et al., 2025; Utama et al., 2026). Crypto-assets were initially positioned as a technological innovation offering efficiency, decentralisation, and transparency in financial transactions. As public interest in crypto investment has increased, however, various associated legal risks have also emerged, particularly cyber-based investment crime. This phenomenon shows that technological development is not always accompanied by adequate legal preparedness and protection (Rizki & Suryokencono, 2023). In a state governed by law, this condition raises concerns about safeguarding the public’s legal interests, especially those of investors vulnerable to fraud and manipulation through digital means (Maksum, 2024; Napitupulu et al., 2025).

Crypto-asset investment crime differs from conventional crime because it is committed through an anonymous and borderless cyberspace and involves complex digital transaction mechanisms (Arnone et al., 2025; Nasir, 2025). Investment fraud, Ponzi schemes, trading-platform manipulation, and the provision of unlawful crypto-assets are forms of technological misuse for unlawful economic gain. These characteristics make crypto-investment crime part of cyber-economic crime, capable of affecting public

confidence and the stability of the economic system. It should therefore be understood not merely as an offense against an individual but as a threat to broader legal interests requiring a comprehensive criminal-law response that adapts to technological development (AllahRakha, 2024; Amoo et al., 2024).

Criminal liability constitutes the normative foundation for enforcing the prohibition of conduct that causes harm to individuals, markets, and the wider economic order. In the context of crypto-asset investment crime, the central issue is not merely whether an unlawful act has occurred, but also whether the conduct can be attributed to a particular offender and whether that offender can be held personally or institutionally responsible. Traditional doctrines of liability face significant limitations when applied to cybercrime, which may involve anonymous actors, complex digital infrastructures, corporations, and other non-traditional legal subjects (Sangalang & Farina, 2023). The use of intermediary platforms, algorithmic systems, pseudonymous accounts, and cross-border transactions can obscure the relationship between the unlawful act, the person who directed or benefited from it, and the resulting harm.

These difficulties are compounded by the need to establish fault, causation, and the identity of the offender in an environment where digital evidence may be dispersed across jurisdictions and controlled by multiple parties (AllahRakha, 2024). Nevertheless, technological complexity cannot, by itself, justify weakening the principles of legality, fault, personal responsibility, and due process. The appropriate response is therefore not to abandon traditional criminal-law principles, but to interpret and develop them in a manner capable of addressing the distinctive methods and organizational structures of cyber-economic crime. A coherent concept of criminal liability must accordingly connect the unlawful crypto-investment conduct, the responsible individual or corporation, the requisite form of fault, and the resulting economic harm. Such a framework is essential to prevent both under-enforcement, in which offenders exploit technological and corporate structures to evade responsibility, and overreach, in which liability is imposed without sufficient proof of legally relevant fault.

Indonesian positive law concerning crypto-assets remains distributed among sectoral statutes and regulations. Crypto-assets are recognised as tradable commodities, but no dedicated rules expressly and comprehensively govern criminal liability for crypto-investment crime. Enforcement commonly relies on general criminal law and cyber law instruments, including the Criminal Code and the Law on Electronic Information and Transactions. This approach often produces debate concerning normative adequacy, legal certainty, and effective protection for victims.

Corporate involvement in crypto-asset trading platforms creates a further issue of corporate criminal liability. Crypto-investment crime may be committed through a business entity or legal person that exploits regulatory gaps and weak supervision. Corporate liability is important to prevent legal subjects from hiding behind a corporate structure to evade criminal responsibility. Its regulation and application to cyber-economic crime, however, still face normative and practical barriers and require closer examination (Sugianto et al., 2025). Furthermore, the rise of decentralized finance and automated smart contracts complicates the attribution of culpability, as the lack of a centralized authority hinders the identification of parties responsible for fraudulent or malicious activities (Pambudi & Fakrulloh, 2025). Current regulatory frameworks often fail to address these systemic organizational faults, as enforcement remains disproportionately fixated on individual offenders rather than the structural negligence of corporate entities (Astuti, 2025).

Crypto-asset investment crime is thus a complex legal phenomenon demanding serious attention. The absence of comprehensive regulation and the underdevelopment of criminal-liability concepts in cyber-economic crime may weaken both enforcement and investor protection. A normative study of criminal liability and Indonesian positive law is therefore necessary. It can contribute to cyber-economic criminal-law scholarship and support recommendations for regulation that responds more effectively to technology-enabled investment crime.

1. How should criminal liability for crypto-asset investment crime be conceptualised within

Indonesia's cyber-economic criminal-law framework?

2. How is criminal liability for perpetrators of crypto-asset investment crime regulated under Indonesian legislation?

METHOD

Normative legal research is doctrinal research, also called library research or document study. It uses legal materials such as legislation, judicial decisions or orders, contracts and agreements, legal theory, and scholarly opinion. This study uses normative legal research to examine criminal liability for crypto-asset investment crime from the perspective of Indonesian cyber-economic criminal law. The method is appropriate because the analysis focuses on legal norms, principles, and doctrines concerning crypto-investment crime and the regulation of criminal liability in Indonesia's positive-law system.

The study applies statutory and conceptual approaches. The statutory approach examines relevant law, including Law No. 20 of 2023 concerning the Criminal Code, Law No. 11 of 2008 on Electronic Information and Transactions and its amendments, and regulations treating crypto-assets as commodities. The conceptual approach examines concepts of criminal law, criminal liability, economic criminal law, and cybercrime found in legal doctrine and literature.

The materials comprise primary, secondary, and tertiary legal sources. Primary materials include relevant legislation and judicial decisions. Secondary materials include textbooks, scholarly journals, and academic writings on criminal and cyber law. Tertiary materials, such as legal dictionaries and encyclopaedias, support the analysis. All materials are analysed qualitatively through deductive legal reasoning to produce systematic and coherent conclusions.

RESULTS AND DISCUSSION

The Concept of Criminal Liability for Crypto Asset Investment Crime

From the perspective of cyber-economic criminal law, crypto-asset investment crime represents a development of economic crime that uses information technology as its principal means. It seeks unlawful gain and may also have systemic effects on public confidence and the stability of the digital economy. Criminal law must respond adaptively to the non-conventional, technology-based, and cross-jurisdictional characteristics of such crime. Liability must therefore be situated in a cyber-economic criminal-law framework integrating criminal, economic, and information-technology dimensions. This approach allows liability to serve preventive as well as repressive purposes in a rapidly changing field (Eddine & Liouarim, 2024; Katyal, 2001).

Conceptually, criminal liability is the legal mechanism for determining whether a person or entity may be held responsible for a criminal act. Under Indonesian criminal law, liability requires an offence, fault, and the offender's capacity to be held responsible (Saleh, 1983). This concept was largely developed for conventional offences committed directly by individuals. In crypto-investment crime, however, offenders often operate through digital systems, anonymous identities, and complex technological infrastructure. The meaning and application of criminal liability must consequently remain responsive and effective while respecting legality and legal certainty (Pambudi & Fakrulloh, 2025).

Crypto-investment crime may be classified as economic crime because it involves the unlawful collection and management of public funds. It abuses public trust and manipulates the digital economy for private or collective gain (Arnone et al., 2025; Nagy, 2025). It can harm individual victims and disrupt economic order and national financial-system security. Liability should therefore protect broader public and national economic interests, not only individual interests. Crypto-investment crime should be treated as cyber-economic crime requiring a specialised response rather than merely an ordinary offence (Putra, 2025).

Fault, or *mens rea*, is central to determining liability. Crypto-investment crime is generally committed

intentionally, whether through direct intent or awareness of the probable consequence. Offenders knowingly design and operate unlawful schemes for illegal gain. Complex digital systems, however, may make fault difficult to prove, especially where online platforms involve many actors (King et al., 2019). Investigators and prosecutors need evidentiary methods adapted to cybercrime without reducing criminal standards of proof. Fault remains the foundation of liability, but its application must reflect the cyber-economic context (Ar et al., 2024).

Potential legal subjects include corporations as well as individuals. Crypto-investment crime may be committed through a company or corporate digital platform. Modern criminal law recognises corporate liability where an offence is committed for the corporation's benefit and within the authority of its management (Manullang et al., 2025). In cyber-economic criminal law, corporate liability prevents legal entities from being used as instruments of digital economic crime. Responsibility should attach not only to individual offenders but also to corporations benefiting from the offence.

Applying corporate criminal liability requires clarity about the governing doctrine. Identification theory and vicarious liability may attribute fault to a corporation through the conduct of its managers or persons controlling its operations. In cyber-economic crime, these doctrines must be capable of addressing complex corporate structures based on digital technology. Without clear rules, corporations may exploit regulatory gaps and technological complexity to evade liability. Stronger corporate-liability principles are therefore essential to effective enforcement.

Crypto-investment crime also creates questions concerning *locus delicti* and *tempus delicti*. Cyber offences frequently lack clear geographical boundaries, making it difficult to determine the competent jurisdiction. This affects enforcement and legal certainty. Cyber-economic criminal law must address jurisdiction flexibly, including through international cooperation and a limited form of universal jurisdiction. Liability for crypto-investment crime therefore has a transnational dimension requiring cross-border coordination (Djunarjanto et al., 2025).

Evidence is another major challenge. Electronic evidence, digital transactions, and encryption require specialised law-enforcement capabilities. Proof can no longer depend only on conventional evidence but must include legally valid and reliable digital evidence (Arifatunnisa & Wiraguna, 2026). The criminal-liability framework must be supported by evidentiary rules and capabilities adapted to technology. Without adequate proof, substantive liability provisions may be ineffective in practice.

Liability must also respect justice and proportionality. A criminal sanction should correspond to the offender's fault and the scale of harm. In cyber-economic crime, punishment should not only penalise the offender but also restore public trust and prevent repetition. Fines, additional penalties, and confiscation of criminal assets are particularly important because crypto-investment offences pursue economic benefit.

Criminal liability is the responsibility borne by a person who commits an offence. An offender may be punished only where statutory elements are satisfied. Liability for crypto-investment crime also performs a preventive function. Clear rules and enforcement can deter potential offenders and improve compliance in digital investment activities. This is increasingly important as technology develops rapidly and public interest in crypto investment grows. Without firm regulation and enforcement, crypto-investment crime may continue to expand and harm society. Liability should accordingly function as an instrument of social control in the digital economy (Suyanto, 2018).

The concept must also align with investor protection. Cyber-economic criminal law does more than punish; it should provide justice to victims. Liability mechanisms should allow recovery of victims' losses through available legal procedures. Criminal law should operate alongside other legal instruments to provide comprehensive protection for crypto-asset investors.

In summary, criminal liability for crypto-investment crime requires a comprehensive, adaptive

approach oriented toward protection of public legal interests. It must extend to individuals and corporations while accounting for complex, cross-border cybercrime. Strengthening the concept and implementation of liability is therefore a prerequisite for effective Indonesian enforcement.

Regulation of Criminal Liability Under Indonesian Legislation

Indonesia has not yet consolidated the regulation of criminal liability for crypto-asset investment crime into a single comprehensive statute. Crypto-assets were initially regulated administratively and commercially as digital commodities, while criminal aspects continue to depend on general criminal-law and cyber-law instruments. This creates a gap between evolving investment practices and regulatory preparedness and may produce uncertainty for both law-enforcement authorities and investors. It is therefore necessary to assess whether positive law provides an adequate basis for cyber-economic criminal enforcement (Mulyana et al., 2025).

Law No. 20 of 2023 concerning the Criminal Code, as general criminal law, may provide a principal basis for addressing crypto-investment crime. Provisions on fraud, embezzlement, and unlawful conduct may be used against offenders. Applying the Criminal Code to cyber-economic crime is nevertheless limited because its relevant offences are framed around conventional conduct. It does not expressly address blockchain technology and digital transactions, producing debate over whether existing offence elements and norms are sufficient. Progressive legal interpretation or regulatory reform is therefore needed to address technology-based investment crime (Rizki & Suryokencono, 2023).

Law No. 11 of 2008 on Electronic Information and Transactions and its amendments also provides an important instrument. It supplies a basis for prosecuting unlawful conduct through electronic systems, including dissemination of misleading information and manipulation of digital data. Its provisions are frequently used where offenders use electronic media to commit crypto-investment fraud. The Law, however, focuses on conduct in cyberspace rather than the economic characteristics of large-scale fundraising and financial loss. Although relevant, it does not fully capture crypto-investment crime as a complex form of cyber-economic crime.

Crypto-assets are also regulated as commodities within the legal framework for commodity futures trading. They may be lawfully traded when applicable requirements are satisfied. From a criminal-law perspective, this regime emphasises licensing, supervision, and administrative sanctions (Simbolon & Sinaga, 2022). It does not expressly establish criminal liability for conduct that causes investor losses. Enforcement consequently remains dependent on general provisions in the Criminal Code and Electronic Information and Transactions Law. This sectoral framework has not yet been integrated with cyber-economic criminal law, limiting enforcement effectiveness (Mulyana et al., 2025).

Supervisory bodies also play a decisive role in determining the effectiveness of criminal liability. Crypto-asset trading is primarily supervised through administrative mechanisms intended to ensure licensing, compliance, and market integrity. However, administrative oversight alone cannot adequately address illegal investment schemes that operate outside the registered system, conceal their activities through digital platforms, or exploit gaps between regulatory jurisdictions. Criminal law should therefore operate as an *ultimum remedium* where violations involve deliberate deception, substantial investor losses, systemic risks, or serious harm to public legal interests. This does not mean replacing administrative supervision with criminal enforcement; rather, the two mechanisms must operate in a coordinated manner. Effective information-sharing, referral procedures, and delineation of institutional authority are necessary to ensure that regulatory violations are promptly detected, appropriately classified, and prosecuted when they attain criminal significance. Without such coordination, offenders may exploit the separation between administrative and criminal regimes, while victims may be left without effective protection or recovery.

Regulation must also address corporations as legal subjects. Although Indonesian positive law recognises corporate criminal liability in several sectoral statutes, its application to crypto-investment

crime remains underdeveloped. This gap is particularly significant because crypto-investment schemes may be organised through corporate structures, allowing decision-making, control, and criminal conduct to be dispersed among the corporation, its directors, managers, and agents. Existing provisions do not clearly establish how corporate fault should be proved where unlawful conduct is facilitated by automated systems, decentralised operations, or complex digital transactions. Without clearer rules on attribution, managerial responsibility, and the relationship between corporate benefit and individual conduct, corporations involved in illegal crypto investment may exploit regulatory uncertainty to evade liability. More explicit corporate-liability rules are therefore necessary to ensure that corporate structures cannot be used to conceal responsibility and to make cyber-economic criminal enforcement effective.

Evidentiary issues present a further challenge to the enforcement of criminal liability. Although Indonesian criminal procedure recognises electronic evidence, the existing framework requires stronger and more specific mechanisms for crypto-investment cases. The pseudonymous, decentralised, and encrypted character of crypto transactions can obscure the identity of offenders, the origin and movement of assets, and the connection between digital conduct and investor losses. Establishing criminal liability therefore requires specialised expertise in blockchain analysis, digital forensics, and the preservation and authentication of electronic evidence. Investigators and prosecutors must also be able to demonstrate the continuity and integrity of transaction records so that blockchain data can be reliably linked to particular persons, accounts, devices, or corporate entities (Atlam et al., 2024; Dhillon et al., 2025; Ponnusamy et al., 2025). Without clear evidentiary standards, adequate forensic capacity, and effective procedures for obtaining and presenting digital evidence, substantive criminal provisions may remain difficult to apply and convictions may be undermined. Strengthening the evidentiary framework is consequently essential to ensure that the legal recognition of criminal liability produces effective enforcement rather than merely formal accountability.

Positive law must also address the transnational dimension. Many crypto offences involve offenders or infrastructure outside Indonesian territory. Liability cannot then depend solely on national jurisdiction. Cross-border rules and international cooperation are indispensable, yet Indonesian law has not systematically accommodated these needs. Reform should integrate national cyber-economic criminal law with relevant international regimes.

International cooperation is indispensable to combating crypto-related cybercrime because offenders, victims, digital platforms, exchanges, and assets may be located in different jurisdictions. States must therefore establish effective mechanisms to identify, trace, freeze, confiscate, and recover illicit crypto-assets, while securing evidence that can be used in criminal proceedings. Cross-border enforcement should not be limited to the exchange of general information; it must also facilitate expedited mutual legal assistance, coordinated investigations, the preservation of electronic evidence, and the extradition or prosecution of suspects. These measures are essential to prevent offenders from exploiting jurisdictional boundaries and to ensure that criminal liability can be enforced in the countries affected by their conduct. International organisations such as Interpol and Europol can support this process by providing platforms for intelligence exchange, joint investigations, operational coordination, and capacity-building among national law-enforcement authorities (Sangalang & Farina, 2023). For Indonesia, strengthening cooperation with foreign regulators, law-enforcement agencies, cryptocurrency exchanges, and international organisations is particularly important because the effectiveness of domestic criminal enforcement may otherwise be undermined when offenders or relevant digital evidence are located abroad.

Criminal law must provide justice to victims as well as punish offenders. Sanctions should reflect the degree of fault and magnitude of loss. Financial sanctions, including fines and confiscation of criminal assets, are highly relevant to cyber-economic crime. Indonesian positive law, however, has not yet formulated a specific and coherent sanctions regime for crypto-investment crime. The present sectoral and partial rules require harmonisation within a comprehensive cyber-economic criminal-law framework

to ensure legal certainty, consistent enforcement, and effective liability (Kaban & Kholiq, 2025).

Indonesia's positive-law framework still requires substantial normative strengthening. The absence of specific, integrated regulation prevents optimal enforcement against crypto-investment crime as cyber-economic crime. Regulatory reform and consolidation are urgent if Indonesia is to respond effectively to digital investment crime and provide meaningful protection to the public.

CONCLUSION

First, crypto-asset investment crime forms part of cyber-economic crime and is characterised by technical complexity, cross-border operation, and reliance on digital technology. Criminal liability may be imposed on individuals and corporations on the basis of fault and corporate-liability principles. Applying those principles nevertheless presents challenges involving proof, offender identification, and the complexity of the technology used in crypto-asset transactions. Second, Indonesian regulation of criminal liability for crypto-investment offenders remains partial and dispersed among several statutes and regulations. Existing instruments, including the Criminal Code and Electronic Information and Transactions Law, do not specifically and comprehensively regulate crypto-investment crime as cyber-economic crime. Enforcement therefore does not yet provide optimal legal certainty, deterrence, or effective investor protection. Stronger, harmonised regulation is needed to build a cyber-economic criminal-law regime responsive to the development of crypto investment in Indonesia.

REFERENCES

- AllahRakha, N. (2024). Cybercrime and the legal and ethical challenges of emerging technologies. *International Journal of Law and Policy*, 2(5), 28–36. <https://doi.org/10.59022/ijlp.191>
- Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, 21(2), 205–217. <https://doi.org/10.30574/wjarr.2024.21.2.0438>
- Ar, A. M., Wirda, W., Rusbandi, A. S., Zulhendra, M., Bahri, S., & Fajri, D. (2024). Peran niat (mens rea) dalam pertanggungjawaban pidana di Indonesia. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3), 240–252. <https://doi.org/10.71153/jimmi.v1i3.140>
- Arifatunnisa, S., & Wiraguna, S. A. (2026). The status of electronic evidence in civil-case proof following the implementation of digital courts. *Media Hukum Indonesia*, 4(1), 365–374.
- Arnone, G., Scire', G., & Bivona, E. (2025). The (mis)use of cryptocurrencies by criminal organizations: A systematic literature review. *Digital Finance*, 7(4), 815–851. <https://doi.org/10.1007/s42521-025-00148-1>
- Astuti, N. K. (2025). Corporate criminal liability in digital economic crimes: An analysis of legal developments in Indonesia. *Indonesian Journal of Law and Justice*, 3(2), Article 9. <https://doi.org/10.47134/ijlj.v3i2.5013>
- Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, 13(17), Article 3568. <https://doi.org/10.3390/electronics13173568>
- Dhillon, D., Mehla, V. K., & Singh, S. (2025). Blockchain-based digital forensics: Methodologies, tools, and future directions. In *Blockchain and cyber forensics* (pp. 231–250). Auerbach Publications. <https://doi.org/10.1201/9781003482154-14>
- Djunarjanto, A. A., Purwati, A., & Marina, L. (2025). Transformasi modus kejahatan ekonomi transnasional di era digital: Analisis hukum pidana dan teknik forensik siber. *SENTRI: Jurnal Riset Ilmiah*, 4(8), 1346–1360. <https://doi.org/10.55681/sentri.v4i8.4448>
- Eddine, M. I., & Liouarim, W. (2024). Combating illegal electronic speculation between the two specialized penal poles: Cybercrime and economic-financial crime. *Journal of Law Society and Authority*, 13(1), 175–194. <https://doi.org/10.52919/ljsa.v13i1.242>

- Kaban, K. S., & Kholiq, A. (2025). Optimising criminal regulation of asset confiscation for economic crime from the perspective of just progressive law. *Jurnal Locus Penelitian dan Pengabdian*, 4(5), 1811–1823.
- Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review*, 149(4), 1003–1114. <https://doi.org/10.2307/3312990>
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2019). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26(1), 89–120. <https://doi.org/10.1007/s11948-018-00081-0>
- Maksum, M. (2024). Legal implications of civil and criminal law on investment fraud under the guise of online business. *Indonesian Economic Review*, 4(1), 29–42. <https://doi.org/10.53787/iconew.v4i1.53>
- Manullang, H., Fernando, Z. J., & Nur, A. I. (2025). Blockchain and corporate criminal liability: Law reform and the technological revolution in corporate accountability. *Journal of Law and Legal Reform*, 6(3), 1411–1450. <https://doi.org/10.15294/jllr.v6i3.22472>
- Mulyana, S. P., Sumaragatha, I. G. B. S., & Evangelista, B. (2025). Urgensi integrasi kewenangan OJK dan Bappebti dalam pengaturan investasi aset kripto di Indonesia. *Jurnal Risalah Kenotariatan*, 6(1), 238–245. <https://doi.org/10.29303/risalahkenotariatan.v6i1.356>
- Nagy, B. G. (2025). Invisible money, visible crime? The emergence of cryptocurrencies in economic crime. *Belügyi Szemle*, 73(11), 2361–2372. <https://doi.org/10.38146/bsz-ajia.2025.v73.i11.pp2361-2372>
- Napitupulu, J. H., Panggabean, M. L., Panjaitan, H., & Widiarty, W. S. (2025). An integrated legal framework for digital investment fraud prevention in Indonesia. *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 3(3), 540–567. <https://doi.org/10.53955/jsderi.v3i3.154>
- Nasir, W. (2025). *Cryptocurrency fraud and financial crime: Analyzing convicted fraudsters in digital asset scams* [Preprint]. Authorea. <https://doi.org/10.22541/au.174180456.65670202/v1>
- Pambudi, P., & Fakrulloh, Z. A. (2025). Criminal liability of perpetrators in crypto ecosystem, the regulatory challenges, and legal voids in the criminal law system in Indonesia. *Majelis*, 2(3), 105–125. <https://doi.org/10.62383/majelis.v2i3.1042>
- Ponnusamy, V., Manickam, N., & Arivazhagan, N. (2025). Blockchain technology for evidence integrity. In *Emerging technologies in digital forensics and cyber security* (pp. 23–42). IGI Global. <https://doi.org/10.4018/979-8-3693-9405-2.ch002>
- Putra, A. A. G. K. (2025). Criminal liability for illegal crypto asset investments in Indonesia. *Journal Equity of Law and Governance*, 7(2), 116–122. <https://doi.org/10.22225/elg.7.2.2025.116-122>
- Rizki, F., & Suryokencono, P. (2023). Pertanggungjawaban penyelenggara investasi bodong yang memakai skema Ponzi dengan modus investasi cryptocurrency. *Indonesian Journal of Law and Justice*, 1(2), Article 10. <https://doi.org/10.47134/ijlj.v1i2.2013>
- Saleh, R. (1983). *Perbuatan pidana dan pertanggung jawaban pidana: Dua pengertian dasar dalam hukum pidana*. Aksara Baru.
- Sangalang, R. S., & Farina, T. (2023). *Reference book on cyber criminal law*. Media Penerbit Indonesia.
- Simbolon, A., & Sinaga, D. I. G. (2022). The legality of cryptocurrency transactions in Indonesia. *Jurnal Daulat Hukum*, 5(3), 196–205. <https://doi.org/10.30659/jdh.v5i3.26722>
- Sugianto, F., Herawati, E., Mustopa, H., Sander, M., & Fujianti, P. J. (2025). Analisis yuridis terhadap tanggung jawab korporasi dalam tindak pidana kejahatan luar biasa di bidang ekonomi. *Jurnal Sosial Teknologi*, 5(7), 2819–2831. <https://doi.org/10.59188/jurnalsostech.v5i7.32225>
- Suyanto. (2018). *Introduction to criminal law*. Deepublish.
- Utama, A. P., Noerdajasakti, S., & Afandi, F. (2026). Legal and criminological analysis of cryptocurrency money laundering in Supreme Court Cassation Decision. *Yurisdiiksi: Jurnal Hukum*, 21(4). <https://doi.org/10.55173/yurisdiiksi.v21i4.345>