GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3

Criminal Liability of Individuals and Third Parties in Crypto-Asset-Based Fraud Schemes: A Dormant Responsibility Perspective

Herwansi Tambunan[1], Megawati Barthos[2]
[1]Universitas Borobudur, Jakarta, Indonesia, herwansit@gmail.com
[2]Universitas Borobudur, Jakarta, Indonesia, megawati_barthos@borobudur.ac.id

Corresponding Author: herwansit@gmail.com[1]

Abstract: The rapid growth of crypto assets in Indonesia has opened up economic opportunities while simultaneously raising the risk of fraudulent activities, such as rug pulls, fake investment offers, and market manipulation, which are detrimental to the public. This study analyzes the criminal liability of individuals and third parties in crypto-based fraud, emphasizing the concept of dormant responsibility, which is criminal liability arising from the negligence or passivity of parties who should have prevented the crime. The method used is normative juridical with a conceptual and legislative approach, examining the Criminal Code, Law Number 1 of 2024 concerning ITE, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, as well as regulations on the crypto asset sector under the supervision of the OJK through POJK Number 27 of 2024. The results of the study indicate that individual perpetrators can be held accountable based on the fraud provisions in the Criminal Code and Article 28 paragraph (1) of the ITE Law, while third parties, such as crypto exchanges, smart contract developers, and custodian service providers, are potentially liable if proven negligent in their supervisory obligations, KYC/AML, or prevention of suspicious transactions. The concept of Dormant Responsibility offers a new normative framework that places active and passive negligence as important elements to close legal loopholes, while balancing consumer protection with technological innovation. Research recommendations include strengthening preventive obligations on crypto service providers, harmonizing criminal regulations with digital financial regulations, and developing technical guidelines for proving crypto assets in court.

Keywords: Criminal Liability, Crypto Assets, Fraud, Third Parties, Dormant Responsibility

INTRODUCTION

The growth of crypto assets in Indonesia is inextricably linked to rapid global developments (Nuryanto, 2021). In recent years, crypto has become a popular investment instrument, attracting interest from the public, especially the younger generation interested in digital technology (Azizul, 2025). The value of crypto transactions in Indonesia continues to

increase, indicating that people are beginning to view crypto as a promising alternative asset (Hartono, 2022). However, this surge in growth has brought new consequences for the legal system, as the potential for misuse of crypto assets for illegal activities is also increasing (Amrullah, 2024). This phenomenon raises the urgent need to regulate and monitor the circulation of crypto to prevent widespread losses.

Crypto assets are not only economic instruments but also a new medium that opens up opportunities for crime with patterns that differ from conventional crimes (Umar, 2024). Crypto-based fraud is usually conducted using methods such as rug pulls, which involve unilaterally withdrawing funds after the victim has invested (Zhou, 2024). Another common form of fraud is fraudulent investment offers with promises of high returns that never materialize (Tambunan, 2022). Market manipulation, such as pump and dump schemes, is also a method that harms retail investors (Siahaan, 2025). All of these methods demonstrate that crypto has vulnerabilities that can be exploited by criminals.

Legal studies of crypto-based fraud are insufficient if they focus solely on individual perpetrators. These crimes involve complex networks involving other parties, both directly and indirectly (Murti, 2024). For example, crypto asset exchange platform providers, software developers, and even custodial service providers can be implicated in cases of negligence. It raises fundamental questions about how criminal law should define the role of third parties with specific legal obligations. Unclear boundaries of responsibility risk creating loopholes that criminals can exploit.

The concept of Dormant Responsibility has emerged as a new framework to address these issues. This term describes a form of criminal liability that focuses not only on active actions but also on negligence or passive attitudes (Michel, 2025). In the crypto world, many parties have a responsibility to monitor and prevent, so silence or inaction can result in significant losses for users (Dharma, 2024). Recognizing this form of responsibility helps broaden the scope of criminal law to be more adaptive to technological dynamics. This way, justice for victims of crypto fraud can be better assured (Mansur, 2023).

The definition of crypto assets in the Indonesian legal system can be found through regulations issued by the government and financial authorities (Rohman, 2021). The Financial Services Authority, through POJK Number 27 of 2024, has taken over the regulatory authority previously held by the Commodity Futures Trading Regulatory Agency (Bappebti) (Utama, 2025). This regulation confirms that crypto assets are recognized as digital financial instruments subject to prudential principles and supervision. This definition is crucial to ensure legal certainty regarding the status of crypto assets, both as investment instruments and as legal objects (Dachi, 2024). Without a clear definition, it is difficult for the law to enforce regulations related to criminal acts involving crypto assets.

The characteristics of crypto assets add to the complexity of their legal regulation. Crypto is decentralized, meaning it has no central authority controlling it (Hasan, 2024). Crypto transactions also offer a high degree of anonymity because they don't always reveal the user's true identity (Chic, 2024). Furthermore, the volatility of crypto prices makes it highly speculative and high-risk (Rolando, 2024). This combination of decentralization, anonymity, and volatility makes crypto vulnerable to being used as a means of crime, particularly fraud. These unique characteristics require the law to adapt to keep up with technological developments.

The elements of criminal liability in Indonesian law always refer to the existence of an unlawful act, fault, and the capacity to take responsibility (Kila, 2023). The newly enacted Criminal Code (KUHP), through Law Number 1 of 2023, maintains this basic principle with adjustments to several articles. Criminal law doctrine emphasizes that a person can only be punished if the elements of fault are met, either intentionally or negligently (Utoyo, 2020). It means the law considers not only the perpetrator's malicious intent but also the possibility of

negligence resulting in criminal consequences. This understanding provides an important foundation for broadening the analysis of crypto crime schemes.

Criminal liability in law is not only directed at individuals but can also be imposed on corporations. Corporations, as legal subjects, can be held accountable for committing crimes or allowing crimes to occur (Tirtawati, 2021). This doctrine is already recognized in various specific laws, including those concerning money laundering and information technology crimes. In the crypto context, service providers that neglect their obligations may be questioned as subjects of liability. It opens up opportunities for the development of new concepts regarding who is considered responsible.

Dormant Responsibility broadens the scope of criminal liability, which has traditionally focused on active actions. Intentional negligence or passivity in situations requiring action are considered equally serious forms of liability. The key elements of this concept include the existence of a legal obligation attached to a particular party, the occurrence of negligence, and the occurrence of harm as a direct result. This understanding emphasizes that inaction in certain circumstances can be as harmful as taking an active, unlawful action. This concept adds flexibility to the criminal legal system in addressing modern crimes.

The position of Dormant Responsibility in contemporary criminal law is increasingly relevant with the development of technology-based crimes. Many cases demonstrate that those who should act as guardians of the system are negligent or reluctant to act (Rinaldi, 2025). Such situations cause significant losses and are difficult to address with legal instruments that only recognize active actions. The concept of Dormant Responsibility provides a normative basis for assessing passive acts as part of criminal liability. Thus, criminal law can adapt to new situations created by technological developments.

The analytical framework used in this study compares the traditional concept of criminal liability with digital-based crimes. Crypto assets present unique characteristics that challenge existing legal mechanisms (Ningsih, 2025). Several criminal law doctrines need to be re-evaluated to avoid a legal vacuum. This analysis also considers how the OJK's established crypto asset oversight regulations can be integrated with criminal law. This integration aims to strengthen the legal framework for crypto-based fraud.

Crypto oversight in Indonesia is a crucial instrument for preventing and prosecuting crime. OJK Regulation No. 27 of 2024 provides the legal basis for stricter oversight of crypto service providers. The regulation stipulates registration requirements, Know Your Customer (KYC) procedures, and reporting of suspicious transactions. This mechanism is expected to minimize the opportunity for fraud and other illegal practices utilizing crypto assets. With proper oversight, public trust in the crypto ecosystem can be maintained while strengthening legal legitimacy in prosecuting violations.

METHOD

The research method used in this study is a normative juridical method, namely legal research that focuses on the analysis of applicable positive legal norms and relevant legal doctrines. The approaches used include a statutory regulatory approach and a conceptual approach. The statutory regulatory approach is carried out by examining various regulations related to crypto-asset-based fraud, including the Criminal Code (KUHP) as amended by Law Number 1 of 2023, Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, and Financial Services Authority Regulation Number 27 of 2024 concerning the organization of crypto-asset exchanges. Meanwhile, the conceptual approach is used to build an analytical framework that not only departs from normative provisions but also interprets and develops a new legal concept, namely dormant responsibility, as a basis for expanding the scope of criminal liability for individuals and third parties. This approach allows research

to go beyond simply describing existing legal regulations to examining principles, fundamentals, and conceptual ideas to address the transnational, anonymous, and complex challenges of cryptocrime. Therefore, this method is expected to yield comprehensive analyses and contribute to the development of cybercriminal law in Indonesia.

RESULT AND DISCUSSION

1. Individual Criminal Liability in Crypto-Based Fraud

Article 378 of the old Criminal Code stipulated that "Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, by deception or a series of lies, induces another person to hand over goods, grant a loan, or cancel a debt, shall be punished by fraud and be punished by a maximum imprisonment of four years." The elements that can be derived from this article include the intent to benefit oneself or another person, the unlawful nature, the use of deception, and the resulting loss to another party. This formulation serves as the basis for prosecuting individuals who use deception in economic activities, including digital-based transactions.

The new Criminal Code, enshrined in Law Number 1 of 2023, adjusts several articles on fraud to make them more modern and relevant to current criminal developments. Article 492 of the new Criminal Code, for example, emphasizes that acts of deception committed to obtain unlawful gain remain categorized as fraud, with updated criminal penalties. The adjustment of terms and the expansion of definitions in the new Criminal Code demonstrate an effort to anticipate criminal modes that are not limited to physical interactions but also encompass virtual transactions. This confirms that the crime of fraud can be applied to crypto-based activities.

The development of crypto assets, characterized by their decentralization and anonymity, does not eliminate the element of fraud. The use of fake whitepapers, promises of unrealistic profits, and the creation of fake applications can be viewed as deception or a series of lies. Losses arising from the public handing over funds in rupiah or crypto assets fulfill the elements of loss as referred to in Article 378 of the Criminal Code. Therefore, even if the medium used is blockchain-based, law enforcement can still prove fraud under the elements of the Criminal Code.

Individual criminal liability in this crime is supported by the principle of fault in criminal law. Perpetrators who deliberately devise a plan to deceive victims through a digital platform clearly have malicious intent (mens rea). The element of unlawful act (actus reus) is fulfilled because their actions actually harm others. These two elements strengthen the legal position that individual perpetrators of crypto fraud deserve criminal responsibility, just as perpetrators of conventional fraud.

Law Number 1 of 2024, the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, emphasizes the prohibition on the dissemination of false information. Article 28 paragraph (1) states: "Any person who intentionally and without authority disseminates false and misleading news that results in consumer losses in Electronic Transactions." This article provides a legal basis for prosecuting individuals who use digital media to deceive the public.

Fictitious crypto investment offers promising multiple returns can be categorized as false or misleading information. Rug pull schemes, where developers withdraw investor funds and then disappear, are also subject to this article, because the information disseminated through whitepapers or social media is misleading from the outset. This article also covers false profit claims that often appear in advertisements for crypto projects without a clear business basis.

The dissemination of misleading information occurs not only through official websites but is also rife on social media, online forums, and instant messaging groups. Fake project

whitepapers designed to lure potential investors can be used as evidence that the perpetrator is spreading false information. When real losses occur to the public, Article 28, paragraph (1) of the ITE Law can be effectively enforced to punish the perpetrator.

Individual accountability is further clarified because this article emphasizes the intentional dissemination of false information. Perpetrators who knowingly create false narratives or spread false claims about crypto assets have fulfilled the elements of a crime. This clarity eliminates the opportunity for perpetrators to hide behind the decentralized nature of crypto technology.

Crypto fraud is often closely linked to money laundering. Proceeds obtained from investors are typically diverted to anonymous wallets, exchanged for other crypto assets, or transferred to foreign exchanges. Law Number 8 of 2010 explicitly regulates this, particularly in Article 2, which lists predicate crimes, including fraud. Therefore, crypto fraud can be a gateway for the application of the Money Laundering Law (TPPU).

Article 3 of the Money Laundering Law stipulates that any person who places, transfers, diverts, spends, pays, deposits, takes abroad, changes the form of, exchanges for currency or securities, or otherwise engages in any act involving assets known to be derived from a criminal act, with the intent to disguise or conceal the origin of the assets, shall be subject to a maximum prison sentence of 20 years and a maximum fine of 10 billion rupiah. This formulation is highly relevant for ensnaring crypto fraud perpetrators who attempt to launder proceeds of crime through blockchain systems.

The Financial Transaction Reports and Analysis Center (PPATK) plays a crucial role in tracking suspicious fund flows. With its authority under Article 40 of the Money Laundering Law, PPATK can request data, analyze transactions, and provide recommendations to law enforcement officials. The transparent nature of blockchain technology allows PPATK to track transaction patterns even if the perpetrator's identity is concealed.

The potential for individual criminal liability is heightened because, in addition to being charged with fraud, the perpetrator can also be charged with money laundering. The combination of these two regulations provides a deterrent effect and strengthens consumer protection efforts. Thus, individuals who commit crypto fraud face multiple criminal threats.

The rug pull scam is one of the most popular forms of fraud. A developer creates a crypto project, offers a new token, and promises extraordinary returns. After the public deposits funds, the developer withdraws all liquidity funds and disappears. This act fulfills the elements of deception and results in real losses for investors, thus categorizing it as fraud under Article 378 of the Indonesian Criminal Code.

Wallet phishing schemes involve tricking victims into providing their digital wallet private keys. The perpetrators typically distribute fake links or fake apps. Once the private keys are obtained, the perpetrators drain the victim's entire crypto assets. The elements of deception, deception, and loss are clearly present in this scheme.

Pump and dump strategies are also frequently used, inflating the token price through massive promotions or controlled buying. After the price soars, the perpetrators sell heavily, resulting in a crash, and other investors suffer losses. This practice is a form of manipulation that involves deception and harms many parties.

Ponzi schemes disguised as crypto are becoming increasingly prevalent, where perpetrators promise fixed returns to existing investors using the funds of new investors. As long as the inflow of funds is steady, these schemes appear legitimate. However, when new investors stop coming in, the scheme collapses, and significant losses occur. Elements of fraud are evident in the false promises and improper allocation of funds.

Each modus operandi demonstrates the fulfillment of the elements of the crime of fraud. The perpetrators use deception, obtain unlawful profits, and cause losses to others. The

diversity of these methods actually reinforces the urgency of law enforcement not to focus solely on one form of fraud, but to encompass all crypto-based variations.

Proving crypto-based fraud crimes faces significant technical challenges. While on-chain crypto transactions are transparent, the perpetrators' identities are often hidden behind wallet addresses. Electronic evidence in the form of smart contracts, blockchain transaction logs, or digital communication recordings becomes crucial for presentation in court.

The perpetrators' anonymity is often a major obstacle. Their true identities can be concealed through the use of VPNs, mixer services, or cross-platform crypto exchanges. Law enforcement efforts must rely on digital forensic techniques to penetrate this anonymity. This demonstrates the importance of law enforcement's capacity to understand blockchain technology.

Crypto transactions also often involve exchanges located overseas. Law enforcement requires international cooperation to obtain data and confiscate assets. Without cross-border support, perpetrators can easily flee their criminal proceeds to less restrictive jurisdictions. This demonstrates the complex global dimension of crypto-based fraud.

The electronic evidence provisions contained in the ITE Law and the Money Laundering Law need to be adapted to the characteristics of blockchain. Article 5 of the ITE Law stipulates that electronic information and electronic documents, along with their printouts, constitute valid legal evidence. However, its application to crypto transactions requires more detailed technical guidelines to avoid doubt in court.

Successful proof is key to ensuring that individual perpetrators are held criminally accountable effectively. Without strong evidence, perpetrators can escape despite significant losses to the public. Therefore, updating evidentiary regulations and increasing the capacity of law enforcement are urgently needed to combat fraud.

2. Third Party Liability and Implementation of the Dormant Responsibility Concept

Third parties in the crypto ecosystem play a crucial role as intermediaries between transaction participants and the system used. Crypto exchanges serve as venues for buying and selling digital assets, facilitating investors and traders. Smart contract developers create automated protocols that can execute specific commands without manual intervention, while custodians provide digital asset storage services with guaranteed security. Payment gateway providers play a role in connecting traditional payment instruments with crypto assets to facilitate smoother transactions. The presence of these various actors expands the reach of crypto assets, while also opening up potential legal risks.

The different roles of third parties carry different legal consequences. Exchanges, as organizers of crypto asset trading, face heavier legal responsibilities because they directly manage the flow of transactions. Smart contract developers are considered system providers who do not always have control over how the contracts are used after they are released. Custodians are obligated to ensure the security of deposited assets, so their negligence can directly impact customer losses. Payment gateways face an obligation to prevent misuse of the payment system, particularly related to illegal transactions or money laundering. The legal standing of each actor determines whether they can be held criminally, administratively, or civilly liable.

Several real-life cases demonstrate the involvement of third parties in crypto-based fraudulent practices. The FTX case in the United States demonstrates how exchanges fail to maintain financial transparency, resulting in significant losses for users. In Indonesia, there have been instances of crypto fraud disguised as investment involving local platforms without official permits, raising questions about the accountability of the providers. Smart contracts have also been exploited in rug pull cases, where developers intentionally withdraw investor funds and abandon projects without clarity. Similar phenomena demonstrate that third parties

not only function as facilitators but can also be actors that increase the risk of crime. These incidents underscore the importance of clear regulations to define the limits of their responsibilities.

OJK Regulation No. 27 of 2024 regulates the operation of crypto asset exchanges by requiring the implementation of KYC principles. KYC implementation aims to identify customers to prevent misuse of digital assets for illicit purposes. Exchanges are also required to implement Anti-Money Laundering (AML) standards and prevent the financing of terrorism through transaction monitoring procedures. Information system security is a crucial requirement to prevent cyberattacks from opening up opportunities for digital asset theft. This regulation demonstrates that financial authorities have begun to position exchanges as institutions subject to prudent principles.

The obligation to report suspicious transactions to the Financial Transaction Reports and Analysis Center (PPATK) is a key oversight instrument. Crypto exchanges must have a monitoring mechanism in place to promptly report any unusual transactions. This information is then used by the PPATK to trace the flow of funds and detect potential money laundering. Failure to report suspicious transactions can result in legal liability, both administrative and criminal. This system emphasizes the role of exchanges not only as business actors but also as partners with the state in preventing financial crimes.

The regulation of crypto asset exchanges is inextricably linked to the Electronic Information and Transactions (ITE) Law and the Money Laundering Law. The ITE Law prohibits the dissemination of misleading information, which often serves as a gateway for crypto fraud, while the Money Laundering Law focuses on illicit fund flows. Payment gateways connected to the banking system are also subject to supervision by the Financial Services Authority (OJK) and Bank Indonesia (BI) to ensure that digital asset transactions do not disrupt national financial stability. This regulatory integration creates a more comprehensive legal framework to minimize technology misuse. The existence of a cross-sectoral legal umbrella is crucial because crypto transactions always intersect with the formal financial system.

International standards also influence the legal obligations of third parties in the crypto ecosystem. The FATF Recommendation mandates the implementation of the travel rule, which requires virtual asset service providers to collect and transmit data on senders and recipients of transactions. This provision is designed to prevent cross-border transactions from becoming a loophole for money laundering. As a member of the FATF, Indonesia needs to adopt this rule into its national regulations to prevent legal arbitrage. Alignment with global standards ensures that crypto exchanges in Indonesia are competitive while adhering to international best practices. This integration also strengthens legal legitimacy in enforcing cross-jurisdictional crypto fraud cases.

Third parties can be held criminally liable if proven negligent, inaction, or active involvement. An exchange that allows anonymous accounts without identity verification could be considered negligent because it creates an opportunity for crime. Smart contract developers who knowingly insert malicious code could also be classified as actively involved in fraud. This type of negligence meets the elements of fault because they have a legal duty to act with due care. The distinction between negligence and intent is key to determining the degree of criminal liability.

The concepts of aiding and abetting describe the role of a third party that knowingly assists in the commission of a crime. A custodian who knows about the storage of assets obtained from crime but continues to provide services could be categorized as an accessory to a crime. Omission liability differs because it refers to a failure to act despite a legal obligation. An exchange that fails to block an account suspected of fraud despite receiving a

warning could be subject to negligence-based liability. Both concepts emphasize that third-party involvement does not have to be an active act but can also be an act of omission.

The principle of "geen straf zonder schuld" emphasizes that there is no crime without fault. Applying this principle requires analyzing whether the third party is truly responsible for the fault. If an exchange has strictly implemented all KYC and AML requirements, but fraud still occurs, it is difficult to impose criminal liability. Conversely, gross negligence can be used as a basis for prosecuting them as a co-responsible party. This principle maintains a balance to prevent arbitrary criminal law from being used.

Administrative and criminal liability often have blurred boundaries in the crypto context. Administrative violations typically result in fines or license revocation, while criminal violations can result in imprisonment. Exchanges that fail to report suspicious transactions may be subject to administrative sanctions, but if proven to have intentionally concealed data, criminal sanctions may be imposed. This distinction requires clear regulations so that business actors understand the risks they face. The lack of clear boundaries has the potential to create legal uncertainty for the industry.

The concept of dormant responsibility arose from the need to regulate third parties who appear passive but actually have legal obligations. Exchanges that allow transactions without KYC can be categorized as parties that remain silent even though they should act. Dormant liability asserts that a party's silence does not absolve them from criminal liability if a causal relationship with the crime is proven. This doctrine provides law enforcement with the opportunity to prosecute those who facilitate crimes through negligence. Its application is particularly relevant in the complex and abuse-prone crypto ecosystem.

The requirements for dormant liability include a legal obligation to act, proven negligence, and a demonstrable causal relationship with the crime. Exchanges that neglect KYC procedures, allowing fraudsters to launder digital money, serve as a concrete example. The duty to act is regulated by the Financial Services Authority Regulation (POJK) and the Money Laundering Law (UU TPPU), so negligence fulfills the necessary legal elements. Evidence of a causal relationship can be traced from blockchain transaction trails that show the flow of funds to the fraudster's account. This evidentiary structure emphasizes that the passivity of a third party does not necessarily mean an exemption from responsibility.

The application of dormant liability faces several serious challenges. The risk of excessive criminalization of business actors can hinder the growth of innovation in the digital finance sector. Many crypto startups are still in the technological experimentation stage, so the threat of criminal penalties can have a counterproductive deterrent effect. Protecting the lex certa principle is crucial to prevent detrimental over-interpretation of the law. Another challenge is proof, as electronic evidence in crypto assets is often anonymous and cross-jurisdictional. Law enforcement requires international cooperation to overcome these technical barriers.

Regulatory reform needs to be directed at harmonizing criminal law with digital finance regulations to avoid overlap. International standards such as the FATF and the travel rule must be adopted to ensure Indonesia remains on track in overseeing crypto assets. Courts also need precise technical guidelines on digital forensics to prove crimes involving crypto assets. Liability models can be expanded, including the application of corporate criminal law or strict liability to prosecute negligent parties. Ultimately, these reforms are expected to strike a balance between consumer protection, legal certainty, and support for the development of financial technology.

CONCLUSION

Individuals involved in crypto-based fraud can be held criminally liable under Article 378 of the Criminal Code concerning fraud and Article 28 paragraph (1) of Law Number 1 of 2024 concerning the Electronic Information and Transactions (ITE) concerning the dissemination of false or misleading information that is detrimental to the public. Various crime methods, such as rug pulls, phishing wallets, and Ponzi schemes, demonstrate that the elements of fraud are met when the perpetrator intentionally misleads the victim to gain profit. On the other hand, third parties, such as crypto exchanges, custodians, or payment gateway providers, may also be held liable if they fail to fulfill their preventive obligations, particularly regarding identity verification, reporting suspicious transactions, and monitoring security systems. The concept of dormant responsibility provides a new normative foundation that broadens the scope of accountability, particularly for parties who appear passive but have a legal obligation to act. This concept closes the legal loopholes exploited in cryptocrime practices, where the main perpetrators and facilitators often hide behind technological complexities and cross-border jurisdictions.

Strengthening regulations and oversight mechanisms is an urgent need to ensure the crypto ecosystem remains healthy and safe for the public. Crypto service providers need to be guided by strict prevention standards through the implementation of KYC and AML principles and reporting to the Financial Transaction Reports and Analysis Center (PPATK). Synergy between institutions such as the Financial Services Authority (OJK), the Indonesian National Police (Polri), the Ministry of Communication and Information Technology (Kominfo), and other law enforcement agencies must be strengthened to address the transnational nature of digital assets. Recommendations for the establishment of specific regulations regarding third-party negligence in crypto asset fraud could provide a new legal basis to define liability limits and prevent excessive criminalization. This research provides theoretical implications for the development of cybercriminal law and provides a conceptual framework that can be used as a reference by policymakers. Therefore, the results of this study are expected to make a tangible contribution to efforts to harmonize national laws with regard to global financial technology developments.

REFERENCES

Amrullah, M. A. (2024). *Inovasi Digital Dalam Bentuk Aset Kripto Sebagai Sarana Untuk Melakukan Tindak Pidana Pencucian Uang. MLJ Merdeka Law Journal,* 5(2), 113–125.

Azizul, A. V. (2025). *Analisis Faktor Minat Mahasiswa Generasi Z Kepulauan Bangka Belitung Dalam Melakukan Investasi. Jurnal Multidisiplin Ilmu Akademik,* 2(3), 282–294.

Chic, S. A. (2024). *Tantangan Dan Peluang Blockchain Di Era Digital Dalam Bidang Keamanan Data Dan Transaksi Digital. Journal of Comprehensive Science (JCS),* 3(11).

Dachi, F. N. (2024). *Tanggung Jawab Perdata Dalam Transaksi Crypto Asset: Kajian Terhadap Risiko Kerugian Investor. Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora,* 3(2), 69–79.

Dharma, P. C. (2024). *Perlindungan Hukum Terhadap Investor Dalam Transaksi Koin Digital Crypto. Jurnal Konstruksi Hukum,* 5(1), 117–122.

Hartono, S., & Budiarsih, R. (2022). *Potensi Kesuksesan Penerapan Pajak Penghasilan Terhadap Transaksi Aset Kripto Di Indonesia. Jurnal Pajak Dan Keuangan Negara (PKN),* 4(1), 132–146. https://doi.org/10.31092/jpkn.v4i1.1740

Hasan, Z. W. (2024). *Regulasi Penggunaan Teknologi Blockchain Dan Mata Uang Kripto Sebagai Tantangan Di Masa Depan Dalam Hukum Siber. Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara,* 2(2), 55–69.

Kila, F. S. (2023). *Pertanggungjawaban Pidana Tanpa Sifat Melawan Hukum Dalam Perspektif Pembaharuan Hukum Pidana. Jurnal Konstruksi Hukum,* 4(1), 28–34.

Mansur, M. (2023). *Regulasi Cryptocurrency Dan Hak Asasi Manusia. El-Faqih: Jurnal Pemikiran Dan Hukum Islam,* 9(2), 177–198.

Michel, S., & Defiebre-Muller, R. (2024). *When Meta-Organizations Fall Asleep: The Dormancy Process. Scandinavian Journal of Management,* 41(1), 101391.

Murti, T. W. (2024). *Analisa Kebijakan Hukum Terhadap Kasus Koin Kripto Sebagai Bukti Elektronik Tindak Kejahatan Pencucian Uang. Media Hukum Indonesia (MHI),* 2(2).

Ningsih, N. H. (2025). *Hukum Ekonomi Digital: Regulasi Bisnis Di Era Teknologi.* Jambi: PT. Nawala Gama Education.

Nuryanto, U. W., & Pramudianto, P. (2021, October). *Revolusi Digital & Dinamika Perkembangan Cryptocurrency Ditinjau Dari Perspektif Literatur Review.* In *National Conference on Applied Business, Education, & Technology (NCABET)* (Vol. 1, No. 1, pp. 264–291).

Rinaldi, F. A., & Wijaya, B. K. (2025). *Efektivitas Penegakan Hukum Terhadap Tindak Pidana Perbankan: Studi Kasus Pembobolan Dana Nasabah. PENG: Jurnal Ekonomi Dan Manajemen,* 2(2), 3437–3447.

Rohman, M. N. (2021). *Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) Di Indonesia. Jurnal Supremasi,* 1–10.

Rolando, B., Al-Amin, A. A., Rahmat, R., Zuwardi, Z., & Izmuddin, I. (2024). *Memahami Nilai Tukar Kripto Dalam Ekonomi Digital: Pendekatan Investasi Di Masa Kini. COSMOS: Jurnal Ilmu Pendidikan, Ekonomi Dan Teknologi,* 1(6), 560–571.

Siahaan, A. L. (2025). *Tanggung Jawab Emiten Terhadap Investor Dalam Kasus Manipulasi Pasar Modal. PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora,* 4(4), 5990–5995.

Tambunan, D. (2022). *Waspada Investasi Ilegal Di Indonesia. Jurnal Perspektif,* 20(1), 108–114.

Tirtawati, S. D. (2021). *Urgensi Pengaturan Mengenai Pertanggungjawaban Pidana Korporasi Dalam Hukum Pidana Di Indonesia. Gorontalo Law Review,* 4(1), 112–124.

Umar, M. F. (2024). *Penggunaan Mata Uang Digital Sebagai Sarana Transaksi Dalam Perspektif Hukum Di Indonesia. Lex Privatum,* 14(3).

Utama, R. A. (2025). *Perlindungan Hukum Terhadap Konsumen Dalam Perdagangan Aset Kripto Di Bawah Pengawasan Otoritas Jasa Keuangan (OJK). Journal of Science and Social Research,* 8(3), 4000–4008.

Utoyo, M. A. (2020). *Sengaja Dan Tidak Sengaja Dalam Hukum Pidana Indonesia. Lex Librum,* 7(1), 75–85.

Zhou, Y., Sun, J., Ma, F., Chen, Y., Yan, Z., & Jiang, Y. (2024, April). *Stop Pulling My Rug: Exposing Rug Pull Risks In Crypto Token To Investors.* In *Proceedings Of The 46th International Conference On Software Engineering: Software Engineering In Practice*, 228–239.