LEGAL GAPS AND ENFORCEMENT CHALLENGES IN ADDRESSING DIGITAL FRAUD INVOLVING CRYPTOCURRENCIES AS TRADABLE COMMODITIES IN INDONESIA

Darwis Nafi Balkista, Rommy Hardyansah, Didit Darmawan, Pratolo Saktiawan, Rio Saputra

Universitas Sunan Giri Surabaya

Correspondence: darwisnafibalkista@gmail.com

ABSTRACT

This paper critically examines the legal dimensions and institutional response to digital asset fraud in Indonesia, focusing on the ambiguities arising from the classification of cryptocurrencies as tradable commodities rather than lawful means of payment. Using a normative juridical approach and thematic literature synthesis, the study analyzes pump and dump, rug pull, and pyramid schemes within the current regulatory milieu, following the transition of crypto oversight from Bappebti to the Financial Services Authority and Bank Indonesia. The research finds that the lack of statutory specificity and regulatory harmonization impedes law enforcement efforts and undermines investor protection, particularly given the international and adaptive nature of digital asset transactions. Furthermore, systemic legislative gaps, technological lags in enforcement, and insufficiently integrated public education initiatives allow perpetrators to exploit these vulnerabilities. The study advocates for the urgent revision of legal definitions, harmonization of payment and commodity regulation, capacity-building in cross-border cooperation, and the integration of technological tools for detection and prevention. Strengthening legal clarity and institutional capacity is vital for safeguarding market participants and supporting the continued growth of a secure, innovative digital economy in Indonesia.

Keywords: cryptocurrency, law enforcement, regulatory ambiguity, investor protection, cross-border fraud, digital assets, Indonesia.

INTRODUCTION

The rapid proliferation of digital assets has transformed global financial systems with unprecedented velocity, presenting both opportunities and unique legal challenges in the regulation of cryptocurrencies. As a borderless, decentralized means of exchange and investment, cryptocurrencies have presented new complexities in the enforcement of business law, necessitating nuanced regulatory structures that can anticipate and respond to patterns of digital fraud. In the Indonesian legal landscape, this transformation demands the reconfiguration of laws to accommodate the peculiarities of crypto assets, especially in view of practices that exploit legal loopholes. The entrance of digital assets into the mainstream of financial transactions has therefore amplified the demand for unambiguous regulation, particularly as speculative investment and schemes designed to manipulate the market escalate in frequency and diversity (Rahayu et al., 2023).

Digital asset fraud has emerged as an acute issue in contemporary financial technology, as signified by certain manipulative practices such as pump and dump, rug pull, and pyramid schemes. Each of these methods leverages the decentralized, somewhat opaque mechanisms of the blockchain to facilitate illicit activities that evade customary oversight applied to more traditional assets (Agarwal et al., 2024). The allure of significant returns in a short period, combined with massive information asymmetry and inadequate public knowledge regarding digital assets, exacerbates the risks borne by ordinary investors. Regulatory agencies are constantly challenged to devise legal frameworks that sufficiently protect participants without stifling innovation (Negara & Darmawan, 2023).

In particular, Indonesia's experience with digital asset fraud illustrates the complexity of striking a balance between economic growth and consumer protection. While technological adoption is broadening access and participation within the digital economy, regulatory instruments must evolve synchronously, taking into consideration the transnational scope of crypto transactions and the inherent limitations of national jurisdiction. Fraudulent schemes, often perpetuated under the guise of legitimate investment, have engendered significant financial losses and public distrust (Collins, 2022; Vital, 2023). The magnitude and variety of these schemes call for an assessment of both preventative and punitive legal responses.

A profound examination of regulatory responses is warranted, as the nature of digital fraud continues to evolve in sophistication and anonymity. Indonesian authorities have enacted a succession of policies aimed at closing regulatory gaps, including the transition of oversight responsibilities from the Commodity Futures Trading Regulatory Agency (Bappebti) to the Financial Services Authority (OJK) and Bank Indonesia, as mandated by recent statutes (Ali et al., 2023; Ali, Dirgantara, & Darmawan, 2024). However, ambiguity remains in both the substantive provisions and enforcement mechanisms targeting digital fraud schemes. The challenge persists in designing a legal environment that privileges investor protection while accommodating the unique features of the underlying technology (Goldwen & Hutabarat, 2024; Aysa, 2021).

Digital asset fraud, particularly involving pump and dump, rug pull, and pyramid schemes, has become increasingly pervasive in recent years, exposing glaring deficiencies within the prevailing legal system. The pump and dump tactic artificially inflates asset prices through coordinated promotion, only for orchestrators to abruptly sell their assets at a premium, resulting in precipitous losses for uninformed investors. Rug pull operations lure investors into projects with significant promotional activities before the developers abscond with contributed funds, leaving participants with worthless tokens (Ali et al., 2023). Meanwhile, pyramid schemes masquerade as innovative blockchain projects while fundamentally relying on constant recruitment, violating core principles of financial propriety (Agarwal et al., 2024).

The legal response to these schemes has struggled to keep pace with the evolving sophistication of perpetrators. Indonesia has initiated transitionary reforms by delegating crypto oversight from Bappebti to OJK and Bank Indonesia through Law No. 4 of 2023 and Government Regulation No. 49 of 2024, with the expectation of more effective enforcement and consumer protection (Rahayu et al., 2023). Yet, in practice, these regulatory measures are frequently criticized for inadequate detail, limited scope, and insufficient mechanisms for cross-jurisdictional cooperation. The adaptability of digital asset instruments and the lack of comprehensive enforcement procedures further compound vulnerability to criminal exploitation.

Another predominant issue resides in the ambiguous status of crypto assets under Indonesian law. Although cryptocurrencies are recognized as tradable commodities, they do not qualify as legal payment instruments in accordance with currency regulation statutes. As a consequence, there is legal uncertainty whenever digital assets are used in ways that mimic payment systems or investment vehicles subject to tighter scrutiny in the banking and capital market sectors, yet evade traditional regulatory obligations (Vital, 2023). In effect, the dualism in legal classification exposes market participants to heightened risk whilst complicating the investigative and prosecutorial processes for authorities.

From a regulatory perspective, enforcement is hindered by both the decentralized nature of digital assets and the cross-border trajectory of illicit transactions. This limits the efficacy of remedies traditionally available to domestic regulators, and necessitates a paradigm shift towards a more collaborative, harmonized, and technologically attuned legal system. Fragmentation in global and national regulatory standards often enables fraudsters to act with impunity, leveraging the lag in rule-making and enforcement to their advantage (Negara & Darmawan, 2023; Goldwen & Hutabarat, 2024). The ongoing challenge is to enhance statutory clarity and procedural efficacy rather than remain perpetually reactive to technological disruption.

Examining the underlying causes of digital fraud in the cryptocurrency space reveals not only institutional deficiencies but also public vulnerabilities to sophisticated manipulation. Inadequate digital literacy among potential investors allows deceptive marketing tactics, misinformation campaigns, and social engineering to proliferate. Pump and dump schemes are typically powered by orchestrated media campaigns designed to generate hype, exploiting herd mentality and FOMO (fear of missing out) among less-informed retail investors (Agarwal et al., 2024). Rug pull schemes are facilitated by the ease of creating and promoting new digital tokens with little to no regulatory oversight, with ill-equipped investors left to bear the consequences. Existing regulatory architectures have yet to address these behavioral dimensions comprehensively, necessitating efforts to embed consumer education within legal reforms.

The necessity of scrutinizing regulatory responses is accentuated by the swift migration of fraudulent actors across jurisdictions and assets. As regulatory regimes lag behind technological innovation, the lack of harmonized enforcement potentiates the proliferation of cross-border schemes that evade detection and prosecution (Collins, 2022). This dynamic amplifies the risks faced by individuals and institutions within Indonesia, and calls for a legal framework that not only addresses current exploitations but is also future-proofed against emergent threats. The multidisciplinary nature of the problem mandates that legal, technological, and educational strategies are deployed in an integrated manner, with special attention to statutory precision and enforcement resilience.

A salient reason for analyzing this issue is the profound impact on investor confidence and the broader stability of financial markets. The perpetual risk of exploitation through digital asset fraud, unless addressed comprehensively by legal instruments, impedes the realization of economic benefits anticipated from wider cryptocurrency adoption. Instability and public distrust could discourage innovation, exclude ordinary citizens from financial participation, and facilitate capital flight. Effective regulation and enforcement, founded on rigorous normative-legal analysis, thus constitute prerequisites for cultivating a robust digital economy in Indonesia (Rahayu et al., 2023).

Moreover, the criticality of this inquiry is accentuated by the need to ensure congruency between national and international regulatory standards. As digital assets inherently traverse national boundaries, piecemeal or inconsistent rules are likely to exacerbate legal uncertainty and enforcement gaps. The imperative to harmonize domestic legislation with international best practices is therefore an anchor for regulatory effectiveness. Without such alignment, Indonesia is placed at a disadvantage both in preventing fraud and in capitalizing on legitimate digital asset-related economic activities (Aysa, 2021).

The purpose of this research is to critically examine and elucidate the statutory and regulatory shortcomings in the prevention, detection, and prosecution of digital asset fraud in Indonesia especially in light of the organizational transition of regulatory oversight and the ambiguous legal characterization of cryptocurrencies. This investigation also aims to explore how such regulatory ambiguities undermine both investor protection and the project of building a resilient, ethically grounded digital market. The findings are expected to contribute substantively to the discourse on strengthening legal architecture, identifying core gaps, proposing empirically grounded legal advancements, and promoting harmonization with global best practices.

RESEARCH METHODS

This study adopts a qualitative approach, utilizing library research to examine statutory frameworks and scholarly discourse related to digital asset fraud in Indonesia. The qualitative paradigm is particularly suitable for critical normative-juridical inquiry, as it enables an in-depth interpretation of legal documents, doctrinal sources, and policy regulations while systematically capturing the dynamic interplay of doctrine, legislation, and judicial practices (Creswell & Poth, 2018). Literature-based qualitative methodology allows for the identification and critical synthesis of statutory gaps and regulatory ambiguities that are frequently obscured in quantitative or positivist designs.

Data for this research are sourced from legal statutes, government regulations, international standards, peer-reviewed academic journals, and authoritative books on digital law and financial technology. The selection of literature is conducted systematically, guided by thematic coding and relevance to business law analysis of cryptocurrency-related fraud. The process involves extracting regulatory texts and scholarly perspectives, followed by thematic synthesis to construct cross-cutting categories of legal issues, regulatory best practices, and recurring loopholes (Bowen, 2009; Flick, 2018). Such an approach is instrumental in tracing the evolution and effectiveness of both domestic and international policy responses toward emergent forms of digital asset fraud.

The analytical process in this research emphasizes thematic synthesis, enabling the amalgamation of various doctrinal strands and empirical insights to yield a coherent and nuanced understanding. By integrating data from statutes, journal literature, and official regulatory documents, the method provides a robust foundation for exploring interconnections between legal principles, regulatory effectiveness, and practical challenges in enforcement (Yin, 2018). The reliability of the study is ensured by triangulating multiple data sources and closely adhering to established protocols for analyzing legal literature, thereby providing both scholarly rigor and practical insight into the challenges associated with regulating and prosecuting cryptocurrency-related fraud.

RESULTS AND DISCUSSION

Regulatory Clarity and Enforcement against Digital Asset Fraud

The Indonesian regulatory landscape for crypto assets has undergone significant transformation, most notably marked by the transfer of supervisory responsibilities from the Commodity Futures Trading Regulatory Agency (Bappebti) to the Financial Services Authority (OJK) and Bank Indonesia. Despite these changes, the clarity and comprehensiveness of the laws governing digital assets remain problematic, particularly in shielding investors from schemes such as pump and dump, rug pull, and pyramid schemes. As Tantanawong (2024) observed in the comparative context of Southeast Asia, regulatory evolution often trails behind the sophistication of technological developments, exposing unwary participants to systemic risk. The Indonesian case is emblematic of this wider regional pattern, with prevailing laws and enforcement mechanisms struggling to anticipate novel illicit practices rooted in blockchain technology and the anonymity it affords.

While OJK and Bank Indonesia are now vested with more extensive regulatory powers, statutory instruments such as Law No. 4 of 2023 and Government Regulation No. 49 of 2024 do not yet display the granularity required for effective preventative and punitive action. Krishnan et al. (2023) argue that the legislative texts, though well-intentioned, remain broad and fragmented, providing too few specifics on the mechanisms to detect, investigate, and penalize asset manipulation and fraudulent off-chain behavior. For instance, there are no binding protocols for the monitoring of token listings, nor prescriptive procedures for inter-agency coordination in investigating pump and dump operations orchestrated on social media.

Contributing to this regulatory opacity is the classification conundrum that permeates the crypto regulatory regime. Although Law No. 4 of 2023 stipulates the recognition of digital assets as commodities, it does not define their risk profiles or behavioral characteristics in sufficient detail. This inadequate legal taxonomy leaves authorities with insufficient criteria to distinguish between licit projects and fraudulent schemes, resulting in inconsistent or delayed action, particularly against rapidly executed rug pulls that are difficult to trace (Aziz et al., 2023). The lack of a shared, precise definition also creates confusion among investigators and judicial officers, diluting the effectiveness of legal redress when digital market manipulation occurs.

Moreover, the Indonesian digital asset regime lacks well-developed whistleblower protections and transparent reporting mechanisms for suspicious activities, thereby limiting proactive enforcement. Sulistiono et al. (2024) highlight the critical role of clear procedural rules and incentives in empowering users, platforms, and other stakeholders to report suspected instances of fraud at early stages. Without such rules, enforcement agencies must rely on ex post facto investigations, which are often frustrated by the swift transfer of assets across decentralized blockchain networks. Weaknesses in cross-border collaboration further compound this disadvantage, allowing perpetrators to exploit jurisdictional gaps and differential regulatory standards.

The practical challenges of enforcing anti-fraud provisions are sharply illustrated by the mechanics of pump and dump and rug pull schemes. In pump and dump, malicious actors coordinate to artificially inflate asset prices through targeted misinformation campaigns spread via online channels, before liquidating their assets—causing sudden market crashes. Regulators lack the technological and legal infrastructure to conduct real-time surveillance or respond to market anomalies with effective speed (Krishnan et al., 2023). Meanwhile, rug pull schemes capitalize on legal and transactional opacity, as project founders abandon a venture after transferring pooled investor assets to anonymous wallets, evading identification and prosecution through pseudonymity and obfuscation (Goldwen & Hutabarat, 2024).

Notably, while POJK No. 27 of 2024 attempts to regulate digital asset exchanges and establish requirements for transparency and reporting, there are discernible gaps in the specification of due diligence standards for newly listed tokens and ongoing operations. Faridi et al. (2023) note that these rules lack forceful, operationalized mechanisms for verifying the legitimacy or sustainability of crypto projects at the entry level. The absence of routine, independent audits and public disclosures leaves investors vulnerable to misleading representations and the inherently high volatility of unvetted tokens. This insufficiency is compounded by the insufficient legal mandate for platform operators to compensate victims of fraud or facilitate the recovery of lost assets.

Consumer protection remains a major area of concern within the emergent legal regime. Anugroh et al. (2023) document the significant disparity between the number of complaints received versus successfully redressed cases, underscoring the need for a complaints resolution system that is accessible, timely, and effective. Although recent regulations encourage greater cooperation among exchanges and law enforcement bodies, rules regarding restitution and compensation in digital asset fraud cases are still absent or inadequately delineated. This leads to a scenario where victims are often left without viable avenues for redress, inhibiting public trust and impeding market development.

The problem of legal uncertainty is further aggravated by the absence of harmonization between domestic crypto regulations and international standards. Given that most crypto-related fraud is executed through cross-border transactions, Indonesian authorities frequently encounter obstacles when seeking cooperation, mutual legal assistance, or information sharing from foreign regulators and service providers (Oriento et al., 2021). This regulatory fragmentation is exacerbated by uneven state capacities and varied legal definitions, hampering efforts to trace assets or identify beneficiaries in pyramid schemes with international reach. Consequently, regulatory bodies struggle not only to detect and prevent emerging frauds but also to surmount the logistical and legal obstacles to cross-jurisdictional enforcement.

Another exploitable gap is found in digital literacy and public education measures, which have not yet been fully integrated into regulatory mandates. Fitrotinisak et al. (2023) demonstrate that while many retail investors remain susceptible to persuasive fraudulent tactics, public awareness initiatives have yet to catch up with the proliferation of investment platforms. Inadequate legal requirements for investor education and misrepresentation warnings contribute to the ease with which unethical actors entice uninformed victims. Legal reforms, to be effective, must connect mandatory public education programs to policy initiatives in order to shrink the asymmetry between sophisticated scammers and less-informed market participants.

Enforcement agencies are further constrained by technological limitations, as current investigative and prosecutorial tools are ill-equipped to follow assets that move instantly, pseudonymously, and often over privacy-enhancing networks. Mazorra et al. (2022) stress that while machine learning solutions for automated scam detection exist and are gaining traction in some jurisdictions, their implementation in Indonesia is hampered by both legal and infrastructural inertia. This technological lag in the regulatory regime continues to allow perpetrators to remain several steps ahead of investigators, with much illicit wealth remaining unrecovered. Therefore, targeted investment in advanced digital forensic capabilities and ongoing regulatory reform are imperative to improve asset recovery and deter future financial crimes (Prananda, 2024).

Although the regulatory transition from Bappebti to OJK and Bank Indonesia is anticipated to foster a more cohesive legal environment, practical coordination among agencies and alignment with broader market surveillance efforts will take time. Until these structural reforms are fully operationalized and enforced with clarity and precision, the window for opportunistic exploitation by unscrupulous actors persists (Sulaiman et al., 2023). The dichotomy between policy ambition and operational execution exposes substantial swathes of the population to ongoing financial risk, reflecting the need for more meticulous legislative drafting and implementation (Ramadhenta & Priyono, 2024).

Prevailing regulatory frameworks in Indonesia, although undergoing promising reforms, are not yet robust or detailed enough to address the evolving complexity and rapidity of fraudulent practices perpetrated through digital assets. Broad statutory language, uncoordinated enforcement mechanisms, technological lag, and insufficient public education all contribute to persistent vulnerabilities. Administrative ambition must be matched by the timely promulgation of unambiguous rules and a commitment to technological and procedural adaptation.

From a theoretical standpoint, these shortcomings do not arise solely from legislative inertia, but are also symptomatic of the unprecedented pace of innovation in the digital asset sphere. The regulatory system must not only respond to existing threats, but must be proactive, forward-looking, and perpetually adaptive so as to guarantee market integrity and safeguard the interests of participants. The prescriptive and punitive instruments available to law enforcement and regulatory agencies must therefore be augmented with cross-disciplinary strategies, integrating insights from technological and behavioral sciences to address the minutiae of digital asset fraud (Aryadi et al., 2024).

Yet, the onus lies ultimately on lawmakers and regulators to ensure that the legal regime remains clearly articulated, effectively enforced, and synchronized with rapidly shifting realities of global digital finance. Ongoing reform should be informed by empirical research and international best practices, as well as timely feedback from all stakeholders. The law, in this context, must become both anticipatory and resilient, systematically closing any loopholes and reducing the incidence of harm. Continued stagnation imperils both investor protections and the promise of an inclusive digital economy.

Legal Classification, Investor Protection, and Law Enforcement

Ambiguity in the legal classification of cryptocurrency assets in Indonesia generates significant repercussions for both law enforcement and investor protection mechanisms. The regulatory stance that recognizes cryptocurrencies as tradable commodities but not as legal payment instruments engenders a dualism that diffuses legal clarity and disrupts the development of coherent enforcement protocols. Emmert (2023) highlights that regulatory certainty is essential for institutional effectiveness; where ambiguity prevails, actors exploit interpretive vacuums, often to the direct disadvantage of market participants facing cross-border criminal activity. In the Indonesian context, such uncertainty is markedly pronounced, as crypto-related activities often intersect with both commodity trading regulations and elements of financial system oversight, with neither sectoral law providing comprehensive coverage.

The absence of explicit legal recognition of cryptocurrencies as payment instruments, as mandated by Indonesian currency law, leads to a fragmented jurisdictional matrix. Law enforcement agencies encounter obstacles in prosecuting fraud cases that mimic traditional financial scams but are perpetrated through digital means. For instance, when fraud schemes use cryptocurrency tokens in ostensibly lawful commodity trading but in reality function as unlawful schemes, such as unlicensed payment systems or unregistered collective investment contracts, gaps in statutory definition allow perpetrators to evade charges or exploit lenient procedural standards (Ali et al., 2023). This regulatory gap not only impedes the investigative process, but also delays or nullifies restitution for victims, who grapple with uncertain recourse pathways.

The problematic dual status is compounded by the adaptability and international reach of crypto transactions. The lack of binding, comprehensive harmonization between commodity and financial service laws results in overlapping, sometimes contradictory, agency mandates—producing confusion over which authority has legitimate oversight. Sahfitri and Rosmalinda (2024) observe that seamless law enforcement is hindered by inconsistencies in the legal status of cryptocurrencies: investigators and prosecutors struggle to apply existing criminal, anti-money laundering, and consumer protection statutes to assets that do not fit classical definitions of currency, securities, or property. Thus, criminals exploit regulatory gray zones to perpetrate cross-border transactions, further complicating the tracing and recovery of misappropriated assets. This underscores the urgency for clear, unified regulatory frameworks to ensure effective cross-jurisdictional enforcement and enhanced legal certainty in managing crypto-related crimes.

Transactional anonymity, pseudonymity, and technological complexity further amplify enforcement challenges. Baraja et al. (2023) demonstrate that existing rules do not mandate centralized record-keeping or comprehensive disclosure requirements for all crypto transactions and wallet holders. Without uniform reporting and transparency obligations—as are standard in conventional banking and capital market regulation—it becomes arduous for authorities to monitor suspicious activities or aggregate actionable intelligence across borders. This deficiency is distinctly problematic when seeking international cooperation on fraud cases, as perpetrators can swiftly transfer funds to foreign platforms with less robust or divergent governance frameworks.

Investor protection is doubly undermined by the lack of statutory specificity and harmonization. Susanty and Setiawan (2022) indicate that while regulatory texts contain general safeguards against fraud, their enforceability is impaired by vague eligibility criteria for protection, ambiguous restitution processes, and discretionary interpretation among agencies and courts. For example, many investors are deprived of protections afforded under banking or capital market law because their investments, made through digital commodities markets, statutorily fall outside formal definitions of regulated financial products. This regulatory vacuum leaves retail investors particularly vulnerable to both domestic and foreign orchestrated scams.

Procedurally, the classification debate invites delays and disputes in the judicial process. Prosecutors face hurdles in evidentiary presentation: establishing the criminal intent behind digital asset-based transactions is arduous without clear legal standards on what constitutes illegal or fraudulent conduct in the crypto sphere (Mirfandaresky & Kaimuddin, 2022). This complexity is frequently mirrored in civil litigation, where claimants must overcome the burden of proof in cases governed by patchworks of partially applicable statutory rules. Consequently, deterrence is weakened as the cost of prosecution rises and the likelihood of conviction falls.

Complicating matters further is the alignment of domestic with international standards—or the lack thereof. Aryadi et al. (2024) suggest that international coordination is central to combatting schemes perpetrated through global crypto networks. Yet, Indonesia's ambiguous regulatory language impairs its ability to effectively request mutual legal assistance or pursue asset recovery abroad, given that regulatory partners may require strict equivalence or compatibility in legal approaches before acceding to cooperation requests. The resultant lack of harmonization not only fosters safe havens for fraudsters but also deters global exchanges from proactively cooperating with Indonesian authorities.

In addition, regulatory ambiguity enables circumvention by platforms and developers. Mazorra et al. (2022) note that in the absence of clear prescriptive requirements for anti-fraud controls—such as compulsory contract audits, user authentication, and robust dispute resolution mechanisms—platform providers can selectively comply or operate at the margins of the law. Such conduct undermines the integrity of transactional ecosystems, perpetuating both actual harms and a pervasive perception of risk among current and potential investors.

The efficacy of civil and administrative sanctions is also diminished by the lack of clear legal bases for targeting illicit or negligent actors. Rusianto et al. (2023) document how ambiguous law can impede the successful application of asset seizure mechanisms, third-party liability provisions, and even the freezing of accounts or transactional flows. Perpetrators, leveraging jurisdictional uncertainty and platforms operating under different legal regimes, can move assets rapidly, thus neutralizing sanctions enacted by Indonesian authorities or rendering them practically unenforceable by foreign partners.

The recognition of digital assets as tradable commodities without parallel or integrated payment regulations, in summary, serves as a persistent source of legal and practical vulnerability. The cross-sectoral and cross-border nature of crypto commerce necessitates a harmonized and comprehensive legal infrastructure. In the absence of such, the adaptability of digital assets outpaces both legislative drafting and enforcement, diminishing the state’s ability to guarantee security or predictability for any market participant—especially ordinary investors. Consequently, regulatory gaps may be exploited by malicious actors, amplifying risks of financial crime and market abuse. Therefore, proactive legislative innovation and international cooperation are urgently required to create robust safeguards and foster greater confidence in the rapidly evolving digital asset landscape.

In crafting a response to these manifold challenges, some progress is being registered. OJK has issued POJK No. 27 of 2024, regulating digital financial asset trading, and the implementation of regulatory sandboxes under POJK No. 3 of 2024 is intended to test technological innovations in a supervised environment before their market-wide release. Such mechanisms, if effectively enforced, could contribute to greater clarity in legal status and operational requirements for crypto platforms. However, as these reforms are emerging, the transition is incomplete and systemic risks persist until policy clarity is fully achieved and integrated with technological and cross-jurisdictional enforcement.

Addressing the classification quandary would not only strategically fortify enforcement capacity but also build sustained investor trust through transparent, readily enforceable standards. Progress depends on multi-level coordination: reconciling banking, commodities, and capital market regulations, as well as fostering alignment with international anti-fraud frameworks and best practices. Regulatory authorities must heighten vigilance and technical proficiency, ensuring legislation and enforcement adapt as rapidly as innovation and exploitative tactics deployed throughout digital markets.

CONCLUSION

The analysis underscores that Indonesia's current legal treatment of cryptocurrencies as tradable commodities, without their recognition as lawful means of payment, fosters substantial ambiguity within the regulatory apparatus. This ambiguity undermines the effectiveness of law enforcement and diminishes the avenues available for robust investor protection. While significant steps have been taken—such as shifting supervisory authority to OJK and Bank Indonesia, and evolving the statutory landscape—critical gaps persist in legal clarity, enforcement coordination, transparency, and victim restitution. At both doctrinal and practical levels, the inadequacies of statutory articulation allow perpetrators of pump and dump, rug pull, and pyramid schemes to exploit regulatory gray zones and technological asymmetries.

These findings present multidimensional implications for the legal, economic, and social spheres in Indonesia. Without an adaptive, integrated, and clear regulatory framework, public trust in digital asset markets remains undermined, which could in turn restrict economic inclusivity and innovation. The lack of enforceable, harmonized standards jeopardizes investor confidence, incentivizing risk-laden behaviors and empowering exploitative actors. Furthermore, deficiencies in cross-border cooperation and domestic procedural consistency hinder Indonesia's ability to participate effectively in global efforts to combat transnational digital fraud.

To address these critical issues, a multidimensional regulatory reform is required. Priority actions should include revising and harmonizing statutory definitions of crypto assets, integrating payment and commodity regulations, and implementing proactive enforcement strategies that incorporate technological innovation such as automated scam detection. Continued development of educational programs aimed at increasing digital literacy is essential, as is the creation of transparent, accessible complaint and restitution mechanisms for victims. Effective international collaboration is vital to closing regulatory loopholes that incentivize the proliferation of cross-border fraud. Ultimately, aligning Indonesia's statutory framework with international best practices will help ensure resilient, adaptive protection for investors and a stable platform for responsible digital asset innovation.

REFERENCES

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. 2024. Blockchain and Crypto Forensics: Investigating Crypto Frauds. International Journal of Network Management, 34(1), 1-32.

Ali, E. M., Dirgantara, F., & Darmawan, D. 2024. Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia. International Journal of Service Science, Management, Engineering, and Technology, 6(3), 27–38.

Ali, M. F., Imran, S. Y., & Apripari, A. 2023. Penegakan Hukum Pidana Terhadap Praktek Rugpull Ditinjau dari Hukum Positif Indonesia. Hakim: Jurnal Ilmu Hukum dan Sosial, 1(4), 317–328.

Anugroh, Y. G., Hardyansah, R., Darmawan, D., Khayru, R. K., & Putra, A. R. 2023. Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions. Journal of Social Science Studies, 3(2), 89–94.

Aryadi, D. W., Hardyansah, R., Darmawan, D., Saputra, R., Putra, A. R., Negara, D. S., & Maulani, A. 2024. Prosecution on Online Gambling Based on Enforcement of Criminal Law in Indonesia. International Journal of Service Science, Management, Engineering, and Technology, 5(2), 1–6.

Aysa, I. R. 2021. Tantangan Transformasi Digital bagi Kemajuan Perekonomian Indonesia. Jurnal At-Tamwil: Kajian Ekonomi Syariah, 3(2), 140-153.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. 2023. Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. Journal of Social Science Studies, 3(1), 23–28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. 2023. Implementation and Supervision of Personal Data Protection Law on Online Platforms. Journal of Social Science Studies, 3(1), 101–108.

Bowen, G. A. 2009. Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2), 27–40.

Collins, J. 2022. Crypto, Crime and Control. Cryptocurrencies as an Enabler of Organized Crime. Global Initiative Against Transnational Organized Crime, Geneva.

Creswell, J. W., & Poth, C. N. 2018. Qualitative Inquiry and Research Design: Choosing among Five Approaches (4th ed.). SAGE Publications, Thousand Oaks.

Emmert, F. 2023. The Long Arm of the SEC in the Regulation of Digital Currencies. Ind. Int'l & Comp. L. Rev., 33(1), 1-37.

Faridi, F., Darmawan, D., Hardyansah, R., Putra, A. R., & Wibowo, A. S. 2023. Legal Protection for Online-Based Lending Consumers. International Journal of Service Science, Management, Engineering, and Technology, 4(2), 34–38.

Fitrotinisak, I. K., Mardikaningsih, R., Gautama, E. C., Sulani, S., & Vitrianingsih, Y. 2023. Legal Compliance for Consumers in Dealing with Cases of Account Tampering in Digital Banking Services. Journal of Social Science Studies, 3(1), 75–82.

Flick, U. 2018. An Introduction to Qualitative Research (6th ed.). SAGE Publications, Los Angeles.

Goldwen, F., & Hutabarat, R. R. 2024. Pembuktian Penipuan Investasi Mata Uang Kripto dalam Pig Butchering Scam. Legal Standing: Jurnal Ilmu Hukum, 8(3a), 806–817.

Krishnan, L. P., Vakilinia, I., Reddivari, S., & Ahuja, S. 2023. Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models. Information, 14(3), 1-20.

Mazorra, B., Adan, V., & Daza, V. 2022. Do not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection. Mathematics, 10(6), 1-24.

Mirfandaresky, S., & Kaimuddin, A. 2022. Digital Forensik dalam Penyidikan Tindak Pidana Penipuan Online (Studi Kasus di Wilayah Hukum Kepolisian Resor Ponorogo). Dinamika, 28(10), 4605–4622.

Negara, D.S. & Darmawan, D. 2023. Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. Bulletin of Science, Technology and Society, 2(2), 13-19.

Oriento, D. S., Negara, D. S., Putra, A. R., Arifin, S., & Saputra, R. 2021. Risks and Legal Protection in Non-Cash Financial Transactions Through E-Wallets. Journal of Social Science Studies, 3(1), 109–114.

Prananda, A. A. A. S. 2024. Enforcement of cryptocurrency money laundering laws as a digital age crime revolution. International Journal of Law, Justice and Jurisprudence. https://doi.org/10.22271/2790-0673.2024.v4.i2a.120

Rahayu, N., Supriyono, I. A., Mulyawan, E., Nurfadhillah, F., Yulianto, D. R., & Ramadhan, A. Z. 2023. Pembangunan Ekonomi Indonesia dengan Tantangan Transformasi Digital. ADI Bisnis Digital Interdisiplin Jurnal, 4(1), 1-4.

Ramadhenta, M. R., & Priyono, F. J. 2024. Harmonization of Authority in the Investigation of the Financial Services Sector in Indonesia. International Journal of Multicultural and Multireligious Understanding. https://doi.org/10.18415/ijmmu.v11i5.5678

Rusianto, R., Hardyansah, R., & Darmawan, D. 2023. Application of the Elements of Money Laundering Crime in Indonesian Jurisprudence. Bulletin of Science, Technology and Society, 2(3), 44–50.

Sahfitri, A., & Rosmalinda, R. 2024. Penipuan Digital Melalui Tautan Phishing. Jurnal Dialektika Hukum, 6(2), 92–107.

Sulaiman, M., Pakpahan, N. H., & Putra, A. R. 2023. Analysis of the Validity and Effectiveness of Electronic Contracts in Legal Protection of Digital Transactions in Indonesia. Journal of Social Science Studies, 3(1), 41–46.

Sulistiono, D., Hardyansah, R., & Darmawan, D. 2024. The Law's Role in Ensuring the Protection and Security of Bank Customers. International Journal of Service Science, Management, Engineering, and Technology, 6(2), 1–5.

Susanty, M., & Setiawan, E. 2022. Sosialisasi Menghindari Penipuan Digital. Jurnal AKAL: Abdimas dan Kearifan Lokal, 3(1), 41–49.

Tantanawong, N. 2024. Information Problems and Investor Behavior in the Cryptocurrency Market in Thailand. Doctoral dissertation, University of Illinois at Urbana-Champaign.

Vital, L. C. 2023. Crypto-Crime: The Evolution of Criminal Finances Using Digital Assets. Master's Thesis, Utica University.

Yin, R. K. 2018. Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications, London.