Justitia Jurnal Hukum, Vol 10, Issue (2), 2026: 214-231
ISSN: P-2579-9983, E-ISSN: 2579-6380
DOI: https://doi.org/10.30651/justitia.v10i2.31759

Reconstructing Penal Accountability in Crypto Asset Fraud: A Two-Dimensional Matrix Analysis of Digital Financial Crimes

Eddy Sambuaga[1*], Hulman Panjaitan[2], Paltiada Saragi[3], Ahmed Jaber Saleh[4]

[1,2,3] Indonesian Christian University, Indonesia
[4] Warith Al-Anbiyah University, Iraq
* Corresponding Author: esambuaga@gmail.com

Article history
Received : Mei 22, 2026
Accepted : September 12, 2026
Published : October 01, 2026

Abstract

This study investigates the legal protection framework and penal accountability mechanisms for retail investors in crypto-assets. A Two-Dimensional Fraud Matrix was employed to map digital economic crimes along the spectrum of service centralization and dominant operational vectors. The proliferation of decentralized financial assets introduces sophisticated fraud typologies transcending conventional market volatility, encompassing smart contract exploitation, deceptive tokenomics, and orchestrated liquidity drains. Recently enacted Law Number 4 of 2023 concerning Financial Sector Development and Strengthening requires a critical evaluation of existing investor protection mechanisms against these complex vulnerabilities. With a normative legal research design, this study evaluates the structural alignment between positive legal norms and empirical risks across the digital asset ecosystem. The findings demonstrate that vulnerabilities categorize into CeFi-Technical, CeFi-Social, DeFi-Technical, and DeFi-Social quadrants. Existing statutory provisions align strongly with CeFi-Technical risks through traditional administrative compliance. Significant penal accountability gaps remain in addressing DeFi-Technical exploitation and DeFi-Social governance manipulation, where perpetrators exploit pseudonymous structures. Dismantling this structural impunity requires a shift from rigid entity-based administrative supervision to an adaptive penal policy. This reconstructive approach requires targeting the natural or legal persons exercising factual control over decentralized protocols by utilizing cyber law instruments and

advanced digital forensics to ensure comprehensive market integrity and substantive justice.

Keywords: Crypto Asset Fraud; Penal Accountability; Retail Investors; Financial Sector Regulation; Two-Dimensional Fraud Matrix.

INTRODUCTION

The rapid evolution of digital financial technology exerts fundamental implications for how global society stores, transfers, and invests economic value. Among these innovations, the emergence of crypto assets represents a profound paradigm shift from simple peer-to-peer electronic cash systems to a multifaceted digital financial ecosystem encompassing payment tokens, stablecoins, non-fungible tokens, smart contract protocols, centralized finance, and decentralized finance (Wang, 2024). This digital transformation reshapes traditional market architectures, compelling national legal frameworks to adapt to borderless, highly dynamic, and technologically complex asset classes (Dupuis et al., 2023).

A pivotal regulatory milestone in this evolution was marked by the enactment of Law Number 4 of 2023 concerning Financial Sector Development and Strengthening. This legislative instrument officially transferred regulatory and supervisory authority over crypto assets from the Commodity Futures Trading Regulatory Agency to the Financial Services Authority (Dupuis et al., 2023). This institutional realignment marks a fundamental shift from a narrow commodity-trading perspective to an integrated financial market framework centered on market integrity, systemic stability, and comprehensive investor protection.

Despite integrated institutional oversight, the widespread adoption of crypto assets has exponentially exposed retail investors to complex fraud typologies that extend far beyond ordinary market volatility. Fraud risks in this domain encompass exchange infrastructure hacks, custodial insolvencies, smart contract exploits, oracle manipulation, cross-chain bridge attacks, misleading promotional campaigns, wash trading, pump-and-dump schemes, insider listing practices, deceptive tokenomics, and governance capture. These pervasive vulnerabilities threaten the financial well-being of retail participants who often lack the technical expertise or sophisticated risk-management tools required to navigate decentralized environments (John et al., 2023). These manipulative practices transcend mere administrative compliance failures, representing sophisticated digital economic crimes that demand robust penal intervention.

Managing these multi-layered risks is exceptionally challenging due to the structural heterogeneity of the crypto ecosystem, which spans a continuous spectrum between centralized and decentralized structures. In centralized financial structures,

retail investors interact with identifiable legal intermediaries, such as centralized exchanges or custodians, where legal accountability can theoretically be pinned onto specific corporate entities. These centralized entities operate within traditional corporate governance boundaries, making administrative enforcement and regulatory compliance legally feasible under established supervisory frameworks (Salami, 2021). Conversely, in decentralized environments, financial interactions occur through autonomous smart contracts and disintermediated blockchain protocols that lack a clear central counterparty. When fraud or operational failures occur in these distributed digital spaces, retail participants face significant procedural hurdles in establishing legal liability and securing effective post-loss recovery. The absence of an identifiable corporate entity, combined with pseudonymous developer networks and immutable on-chain execution, creates a profound accountability vacuum that challenges the foundational principles of traditional financial consumer protection law and requires the reconstruction of a targeted penal policy.

Previous studies underscore the regulatory complexities governing digital financial assets across major global jurisdictions. Wronka conducted a comparative doctrinal analysis evaluating the regulatory frameworks of the United Kingdom and Germany, highlighting institutional divergence between principles-based oversight and prescriptive, technology-neutral licensing (Wronka, 2024). The study demonstrated that while flexible regulatory environments foster technological innovation and market growth, prescriptive regimes offer heightened investor confidence and legal certainty. Wronka emphasized that persistent regulatory ambiguities regarding asset classification and cross-border compliance continue to challenge both regulatory authorities.

Departing from European regulatory dynamics, van der Linden investigated the anticipated legal certainty and market impacts of the European Union Markets in Crypto-Assets regulation (Van Der Linden & Shirazi, 2023). Using a legal-sociological and doctrinal approach, their research evaluated whether harmonized supervisory rules would accelerate institutional and retail adoption of crypto assets. The findings revealed that broad statutory definitions and complex compliance burdens risk generating legal uncertainty and placing disproportionate administrative pressures on smaller market participants. Thus, the authors argued that regulatory frameworks must balance systemic stability with proportionate innovation incentives.

Addressing the specific vulnerabilities of distributed structures, Wronka examined compliance challenges and financial crime risks inherent within decentralized finance ecosystems (Wronka, 2023). The study analyzed how decentralized protocols work independently of traditional financial intermediaries, creating significant regulatory blind spots for supervisory authorities. The research established that unique decentralized operational models prevent standard enforcement mechanisms from effectively monitoring illicit flows, money laundering,

and investor exploitation. Accordingly, the study stressed the urgent necessity for regulators to design specialized compliance tools tailored to disintermediated digital environments.

Despite the growing volume of scholarly literature on digital asset regulation, existing studies mostly show critical analytical limitations. Traditional legal studies often treat crypto fraud as a homogenous phenomenon or focus narrowly on institutional licensing, anti-money laundering compliance, and centralized platform registration. While essential, these entity-based administrative approaches fail to address the profound operational distinctions between centralized platforms and decentralized protocols. Existing literature also tends to overemphasize technological vulnerabilities while underanalyzing the socio-economic and behavioral vectors of digital fraud. In practice, retail investor losses stem equally from asymmetrical information structures, market manipulation, deceptive narratives, and concentrated governance power. This oversight leaves a significant research gap: no structured analytical tool can map crypto fraud typologies against the adequacy of statutory legal norms and penal accountability mechanisms.

To address this gap, this study introduces the Two-Dimensional Fraud Matrix, a novel analytical framework for evaluating legal protection and criminal liability paradigms for retail crypto asset investors. The analytical framework categorizes crypto fraud risks along two distinct intersecting dimensions encompassing the degree of service centralization along the centralized-decentralized spectrum and the dominant fraud vector along the technical-social spectrum. By systematically evaluating these dimensions, this paper examines how positive legal norms established under domestic financial sector legislation align with empirical ecosystem risks. The evaluation ultimately formulates a reconstructive framework that shifts regulatory oversight from a purely administrative entity-based model to a targeted penal policy and risk-proportionate paradigm based on factual control.

METHODS

This study adopts a normative juridical research design to evaluate the structural adequacy and alignment of positive legal norms governing retail crypto asset investor protection following the enactment of Law Number 4 of 2023 concerning Financial Sector Development and Strengthening (Marzuki, 2019). The central analytical inquiry evaluates statutory frameworks, regulatory mandates, institutional oversight mechanisms, and penal accountability structures rather than observing empirical social behaviors. Given this doctrinal focus, the research relies primarily on normative legal materials, established academic doctrines, and international regulatory benchmarks to construct a rigorous evaluative baseline.

For a comprehensive legal evaluation, the research integrates four distinct methodological approaches within a structured narrative framework. The statutory approach systematically examines primary legal instruments, including Law Number 4 of 2023 concerning Financial Sector Development and Strengthening, Law Number 1 of 2023 concerning the New Criminal Code, Law Number 1 of 2024 concerning Electronic Information and Transactions, and relevant administrative rules governing digital financial assets. Concurrently, the conceptual approach refines the theoretical foundations of criminal liability, factual control, decentralized finance, and the two-dimensional taxonomy of technical versus social fraud. Complementing these foundational analyses, a library-based case approach examines documented crypto fraud incidents strictly to help illustrate risk mapping, while a limited comparative approach benchmarks national digital asset regulations against standards formulated by global supervisory bodies (Efendi, 2022).

The research materials comprise three hierarchical tiers: primary, secondary, and tertiary sources. Primary legal materials consist of binding statutory provisions, legislation, and official regulatory decrees issued by the Financial Services Authority. Secondary legal materials incorporate peer-reviewed journal articles, formal legal treatises, authoritative doctrines, and academic commentaries concerning digital financial regulation, cyber law, and criminal investor protection. Tertiary non-legal materials integrate technical whitepapers, industry publications, digital forensic analytics reports, and international financial organization policy documents to capture rapidly evolving technological fraud vectors accurately (Widiarty, 2024).

The analytical process operates qualitatively, using the Two-Dimensional Fraud Matrix as the primary theoretical perspective through a structured multi-stage pipeline. Empirical patterns of crypto asset fraud are initially identified and classified along the centralized-to-decentralized spectrum alongside the technical-to-social fraud vector spectrum, generating four precise analytical quadrants. A rigorous normative gap assessment then maps these identified risk profiles against positive statutory norms to determine areas of normative alignment, partial coverage, or complete regulatory absence. The analytical stage synthesizes these findings to formulate reconstructive legal recommendations that shift the national regulatory framework from a purely administrative, entity-based model to an integrated penal policy and risk-proportionate regulatory paradigm.

RESULT AND DISCUSSION

Mapping Crypto Fraud Typologies through the MF2D Framework

Conventional financial regulation mostly works on the presumption of identifiable corporate intermediaries subject to strict licensing, capital requirements, and administrative liability. The crypto asset ecosystem operates across a heterogeneous continuum characterized by varying degrees of structural

centralization and distinct operational risk vectors (Barczentewicz & de Gândara Gomes, 2024). The Two-Dimensional Fraud Matrix addresses this complexity by mapping fraudulent conduct along two primary axes: the structural centralization spectrum anchored by Centralized Finance at one pole and Decentralized Finance at the other, and the dominant fraud vector spectrum distinguishing between technical and social manifestations of fraud. These intersecting dimensions create four principal analytical quadrants, encompassing CeFi-Technical, CeFi-Social, DeFi-Technical, and DeFi-Social, which collectively capture the multifaceted spectrum of crypto-related investor harm (Costello & Gundur, 2026).

Within the CeFi-Technical quadrant, fraud risks arise primarily from technological breaches, system failures, and inadequate operational safeguards within centralized service providers. In this domain, retail investors interact directly with identifiable custodial entities, such as centralized exchanges, digital asset custodians, and fiat gateways. Typical risks include exchange infrastructure hacks, hot wallet breaches, inadequate cold storage segregation, custodial insolvencies, and system outage disruptions (Ledoux & Smaili, 2025). From a legal perspective, this quadrant presents the highest degree of normative clarity because centralized service providers serve as incorporated legal entities subject to corporate governance, contractual liability, and administrative oversight under financial supervisory authorities. When a centralized exchange suffers a security breach due to negligent cybersecurity protocols, the legal path for establishing institutional liability is relatively clear.

In contrast, the CeFi-Social quadrant addresses fraud vectors driven by information distortion, market manipulation, and deceptive promotional activities occurring within centralized service environments. In these scenarios, the platform's underlying technological infrastructure may function flawlessly with no technical glitches or security breaches. Nevertheless, retail investors suffer severe economic harm because their investment decisions are intentionally manipulated through artificial market indicators, opaque listing practices, or predatory promotional strategies. Prominent fraud typologies within this quadrant include organized pump-and-dump schemes, wash trading to generate fake liquidity, insider listing practices, undisclosed conflicts of interest between platforms and market makers, and misleading marketing campaigns executed through paid social media influencers. This quadrant highlights a profound information asymmetry between institutional platform operators and retail market participants (Nghiem et al., 2021).

Shifting across the structural axis, the DeFi-Technical quadrant represents a radical structural departure, encompassing fraud vectors and systemic losses originating from vulnerabilities in smart contracts, decentralized protocols, price oracle mechanisms, cross-chain bridges, and automated market maker liquidity pools (Li et al., 2025). Unlike centralized ecosystems, decentralized applications run on

public, permissionless blockchains through autonomous, self-executing code without relying on a centralized corporate intermediary. Major risks in this quadrant include smart contract logic exploits, reentrancy attacks, flash loan price manipulations, governance timelock overrides, and bridge security breaches. The primary legal dilemma here is the profound breakdown of traditional accountability structures. Under classical legal doctrines, establishing liability requires identifying a legal person who owes a duty of care or committed a wrongful act, whereas decentralized protocols are deployed by pseudonymous developers and executed immutably on-chain (Ardia & Bluteau, 2024).

The DeFi-Social quadrant covers fraud vectors stemming from governance manipulation, deceptive tokenomics, false decentralization claims, and community-level information distortion within decentralized ecosystems. In this quadrant, investor losses stem not from software bugs or coding vulnerabilities, but from asymmetrical power structures, opaque governance distribution, and manipulative economic designs disguised as decentralized community projects. Common fraud typologies include rug pulls executed by project founders who retain hidden administrative keys, concentrated governance token distribution allowing insider cartels to vote through predatory protocol changes, and false advertising claiming complete protocol decentralization when factual control remains concentrated among core developers. The legal complexity of this quadrant lies in unmasking pseudo-decentralization, requiring regulatory frameworks to look beyond formal architectural claims and establish factual accountability standards based on practical control over protocol upgrades (Kalacheva et al., 2026).

Documented industry incidents validate the distinct risk profiles within centralized environments. In the CeFi-Technical domain, the catastrophic collapse of prominent global exchanges illustrates how unauthorized commingling of user deposits and a lack of independent cryptographic proof of reserves generate massive retail asset losses. Simultaneous failures in cold storage segregation and internal risk controls allow operational deficits to remain hidden until a liquidity crisis triggers sudden withdrawal freezes. Shifting to the CeFi-Social quadrant, regulatory enforcement actions consistently highlight how high-profile figures and coordinated affiliate networks artificially inflate asset prices through orchestrated social media campaigns. Retail investors who enter the market based on these undisclosed promotional partnerships ultimately absorb institutional insiders' liquidity exits, demonstrating the severe economic impact of manufactured market sentiment.

Within decentralized structures, empirical cases highlight a completely different vulnerability spectrum. In the DeFi-Technical quadrant, forensic reports frequently document the exploitation of flash loan mechanics and reentrancy vulnerabilities, where malicious actors manipulate price oracles to drain automated liquidity pools in a single transaction block. The immutable execution of these smart

contracts ensures that exploited funds cannot be administratively reversed. Regarding the DeFi-Social quadrant, prevalent rug pull schemes provide textbook examples of governance manipulation. Project founders often deploy deceptive tokenomics featuring hidden minting functions or concentrated administrative keys, enabling them to alter protocol rules or liquidate massive token reserves unilaterally. These incidents expose the fallacy of complete decentralization, revealing how pseudonymous developers exploit the guise of community governance to mask centralized economic extraction.

The Two-Dimensional Fraud Matrix reveals that crypto asset fraud inflicts multidimensional harm on retail investors, systematically categorized into direct asset loss, cognitive information distortion, and procedural obstacles to legal recovery. Direct asset loss represents the immediate economic injury manifesting primarily within technical quadrants of both centralized and decentralized ecosystems. In centralized technical environments, asset depletion occurs through infrastructure security breaches, exchange insolvencies, and unauthorized commingling of customer deposits with corporate operational funds. In decentralized technical settings, asset loss stems from protocol-level vulnerabilities, including smart contract reentrancy bugs, price oracle manipulation, and flash loan exploits. Because distributed ledger transactions are cryptographically immutable and executed autonomously on-chain, stolen or drained digital assets cannot easily be frozen, clawed back, or reversed through conventional administrative injunctions (Schuler et al., 2024).

Beyond direct asset depletion, retail investors are heavily impacted by systemic information distortion, which dominates the social quadrants of the matrix. Information distortion undermines the foundational market principle of informed consent by corrupting the data, narratives, and price indicators upon which retail investors rely to make investment decisions. On centralized platforms, this distortion manifests as artificial volume generation through wash trading, insider listing manipulation, and aggressive promotional campaigns spearheaded by paid influencers (Cheraghali et al., 2024). In decentralized environments, information distortion operates through misleading whitepaper representations, deceptive tokenomics, unsustainable yield promises, and governance capture by insider cartels. When projects falsely market themselves as community-governed while insiders retain administrative control, retail participants are lured into high-risk assets under false pretenses (Grobys et al., 2022).

The damage inflicted by asset loss and information distortion is further exacerbated by profound obstacles to legal recovery, representing a systemic failure of post-loss enforcement mechanisms. In centralized structures, although a corporate legal entity is nominally identifiable, retail investors face daunting procedural hurdles, including complex cross-border jurisdictional arbitrage, mandatory

arbitration clauses, and liability limitation disclaimers embedded in platform terms of service agreements. In decentralized ecosystems, these recovery obstacles become virtually insurmountable due to the structural disintermediation of decentralized protocols. The diffusion of administrative influence across pseudonymous developers, governance token holders, front-end interface providers, and liquidity pool creators makes it extraordinarily difficult for courts to assign legal liability under classical doctrines of tort or contract law. Consequently, technological irreversibility, jurisdictional evasion, and anonymous governance leave retail investors isolated in a legal loophole, bearing full financial loss without effective judicial redress or administrative compensation, while structural impunity shields malicious actors and demands targeted penal intervention.

Reconstructing Criminal Liability in Decentralized Financial Fraud

The rapid expansion of decentralized digital assets requires a fundamental shift from administrative oversight to targeted penal policy. Traditional regulatory frameworks rely heavily on entity-based compliance, which proves entirely ineffective when addressing deliberate economic extraction hidden within autonomous smart contracts. The Two-Dimensional Fraud Matrix shows that crimes in the decentralized quadrant fall well outside the reach of pure administrative law (Costello & Gundur, 2026). Manipulative practices such as deceptive tokenomics, hidden governance extraction, and orchestrated liquidity drains transcend ordinary market volatility or organic technological failure. These actions constitute severe digital economic crimes that destroy market integrity and shatter public trust in financial technology innovation. Law enforcement agencies can no longer treat this phenomenon as merely a civil liability failure or an investment risk naturally borne by retail investors. A dogmatic criminal-law approach must be integrated immediately to dismantle the fraudulent architecture hidden behind false narratives of decentralization. Tolerating this accountability gap will only perpetuate structural impunity for new-style white-collar criminals exploiting the lack of a single jurisdiction in cyberspace. Reconstructing penal policy requires a profound understanding that code can be deployed with malicious intent and destructive capacity far exceeding conventional fraud methods. The criminal justice system must adapt quickly to ensure legal protections reach virtual spaces previously considered immune to state jurisdictional intervention. Creating a robust penal system is indispensable for protecting vulnerable retail demographics from highly sophisticated technological exploitation.

The criminal qualification for offenses within decentralized crypto ecosystems already has a strong normative foundation in the national positive legal system. This specific form of crime falls directly within the domain of electronic-based fraud. These matters are explicitly regulated under Article 28, paragraph 1, in conjunction with

Article 45A, paragraph 1 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. This regulation targets those who deliberately disseminate electronic information containing false or misleading notifications resulting in consumer losses in electronic transactions. Applying this statutory formulation is highly relevant to eradicating fake promotions, fictitious profit promises in project whitepapers, and token project engineering in cyberspace, which are often designed from the outset to manipulate retail investors' perceptions. Perpetrators cannot evade justice by claiming that investors consented to algorithmic risks because such consent was obtained through intentionally distorted and concealed material information. Information manipulation in the digital asset ecosystem undermines transparency, a fundamental pillar of consumer protection. This cyber law instrument provides a powerful basis for law enforcement to prosecute the dissemination of false narratives that trigger mass economic losses. This protective legal net ensures that crimes arising from electronic information manipulation can be immediately qualified as serious offenses demanding strict penal sanctions with no room for compromise (John et al., 2023).

Predatory practices within this decentralized space also intersect directly with criminal offenses in the digital financial sector based on Law Number 4 of 2023 concerning Financial Sector Development and Strengthening. Because the supervisory authority over digital financial assets has been fully transferred to the Financial Services Authority, conducting financial activities or managing crypto assets without official authorization, along with market-manipulation practices that harm the public, can be prosecuted under the specific penal provisions of this statute. This comprehensive law expands the reach of state authority to touch shadow activities operating freely outside the regulatory perimeter of traditional banking or capital markets. Criminals who establish fake decentralized exchanges or manage fraudulent liquidity pools are fundamentally engaging in large-scale illegal public fundraising (Carpentier-Desjardins et al., 2025). Integrating penal provisions into this financial sector regulation affirms that all market creation, token minting, and initial coin offering activity must comply with strict reporting integrity standards. Using penal instruments within this umbrella law ensures that supervisory institutions have the structural repressive capacity to prosecute malicious actors hiding behind the complexities of blockchain technology. This proactive measure transforms the supervisory function from a mere administrative record-keeping tool into a tangible law enforcement instrument with coercive power over entities and individuals exploiting the national financial system. Bridging the gap between technological advancement and legal enforcement relies heavily on maximizing these specific sectoral penal provisions (Kalacheva et al., 2026).

Complementing cyber law instruments and sectoral financial regulations, material criminal law can also address general fraud offenses outlined in Law Number 1 of 2023 concerning the New Criminal Code, including fraudulent acts and commercial fraud. Modern material criminal law recognizes that deceitful practices are no longer limited to face-to-face interactions or forgery of paper documents. Deploying smart contracts intentionally embedded with malicious code or decentralized structures specifically designed to deceive retail investors fully satisfies the elements of fraudulent acts under the New Criminal Code. Prosecution through this commercial fraud pathway highlights the crime's true substance: the intent to unlawfully benefit oneself or others by using a false name, false dignity, deceit, or a structured web of lies. Crypto project developers creating anonymous identities to drain public liquidity funds are essentially orchestrating a high-level premeditated crime. The convergence of these three layers of legal foundations creates a multi-tiered normative safety net impenetrable by any alibi of technological sophistication. This legislative configuration shows that the national criminal justice system has the dogmatic flexibility required to respond to the evolving dynamics of modern financial crime. Strengthening this doctrinal foundation allows judges and prosecutors to pursue technological criminals using well-established legal principles adapted for the digital era.

The most fundamental dogmatic challenge in prosecuting decentralized financial crimes lies in setting precise legal subjects amidst a sea of absolute anonymity. Criminal liability absolutely cannot be attached to autonomous smart contracts, passive computer code lines, or decentralized protocols lacking tangible form. A progressive penal policy must pierce the veil of pseudonyms to target the natural or legal persons factually exercising control over the digital ecosystem. This targeted accountability approach applies directly to core project developers, founders secretly holding administrative keys, and insider cartels that manipulate system-governance voting in an organized manner (Trozze et al., 2024). Relying on the factual control doctrine prevents malicious actors from escaping justice merely by labeling a project they unilaterally control as an autonomous community initiative. Law enforcement officers are tasked with the duty to dismantle a project's shadow governance structure to determine which party holds economic authority and the highest technical access to drain assets. Advanced tools such as digital evidence, including crypto wallet movement tracking, cross-border exchange fund flow analysis, and blockchain forensics, are crucial investigative instruments. These cutting-edge tools work scientifically to link criminals' real identities to the anonymous digital addresses used to execute large-scale fraud. Establishing factual control ensures that liability rests entirely with human actors who deploy the technology for malicious purposes.

Prosecuting decentralized financial crime schemes demands meticulous evidentiary standards to establish malicious intent or the perpetrator's subjective element convincingly. Distinguishing premeditated fraud from purely organic technological failure relies heavily on analyzing immutable, unalterable operational track records on the blockchain. Malicious intent becomes glaringly obvious when forensic investigators uncover hidden token-minting functions within the code layers, massive asset accumulation in developer wallets kept out of public view, or aggressive promotional campaigns run immediately before founders unilaterally abandon a project. These recurring structural choices and manipulative behaviors provide irrefutable evidence of a premeditated scheme from day one to extract retail investor capital through a series of lies. Integrating all these penal mechanisms into a comprehensive regulatory matrix demands absolute adherence to the principle of mobilizing the ultimate legal force. Criminalization must function precisely to target deliberate digital power abuse with predatory extraction motives. A calibrated penal policy ensures the legal system can decisively neutralize structural impunity without killing legitimate financial innovation or wrongfully punishing coding errors that lack malicious intent. This holistic approach uniting digital literacy and criminal law rigidity will ultimately harmonize modern financial market integrity with comprehensive constitutional protection for all layers of investors

Evaluating Regulatory Alignment and Reconstructive Strategies

Evaluating the legal framework established under Law Number 4 of 2023 concerning Financial Sector Development and Strengthening and corresponding Financial Services Authority regulations through the Two-Dimensional Fraud Matrix reveals significant normative asymmetry. The strongest degree of normative alignment is concentrated in the CeFi-Technical quadrant. Because centralized service providers, such as registered crypto exchanges and digital asset custodians, operate as incorporated corporate entities within a traditional statutory perimeter, current financial regulations successfully establish binding obligations in institutional licensing, corporate governance, cybersecurity standards, and the mandatory segregation of customer assets (Milunovich & Lee, 2022). Despite this relatively high structural alignment, critical operational gaps remain unresolved. The framework lacks standardized, real-time security breach reporting mandates; mandatory independent cryptographic proof-of-reserves audits; explicit statutory compensation funds for technical failures; and binding post-breach resolution procedures to compensate retail investors affected by system outages or hot wallet compromises (Chen et al., 2023).

The degree of regulatory alignment weakens substantially in the CeFi-Social quadrant, yielding a state of partial normative coverage. While existing legal norms governing financial consumer protection, transparency, and general prohibitions

against market manipulation provide a foundational legal basis, they struggle to address the specific agile mechanics of crypto market conduct. Misconduct in centralized digital asset markets rarely occurs through formal corporate disclosures. Instead, manipulative practices are coordinated across decentralized social media channels, affiliate marketing networks, paid influencer endorsements, and cross-platform promotional campaigns (Trozze et al., 2023). Current statutory frameworks lack specific rules mandating explicit promotional disclosures for paid influencers, strict prohibitions on affiliated market-making, insider listing restrictions, and real-time cross-exchange market surveillance systems capable of detecting algorithmic pump-and-dump schemes. The resulting information asymmetry between institutional platform operators and retail participants remains largely unaddressed by statutory protections.

Shifting to the decentralized domain, current legal norms show severely limited alignment within the DeFi-Technical quadrant. Traditional financial statutes are fundamentally engineered to oversee identifiable corporate entities possessing physical domiciles, board structures, and administrative compliance departments (Jaffri, 2026). These entity-centric frameworks are structurally ill-equipped to regulate autonomous smart contracts, disintermediated liquidity protocols, or cross-chain bridges executing immutably on public blockchains. Although certain intermediary actors surrounding decentralized ecosystems, such as centralized front-end interface providers and commercial access gateways, could theoretically fall within the regulatory perimeter, current legal norms do not define their specific legal liabilities regarding smart contract code vulnerabilities or technical risk disclosures. When protocol-level exploits occur, retail investors remain completely exposed to substantial technological risks without adequate legal protection, administrative oversight, or effective recovery mechanisms (Srifa et al., 2025).

The weakest normative alignment appears within the DeFi-Social quadrant, where positive legal norms fail to address the socio-governance dynamics of decentralized digital asset projects. Current financial regulations lack the conceptual and normative tools to address governance token concentration, misleading tokenomics designs, insider voting cartels, and fraudulent claims of protocol decentralization. Many decentralized projects market themselves as fully community-controlled, yet practical control and economic extraction frequently remain concentrated among pseudonymous project founders or early venture capital insiders (Charamba et al., 2025). The legal framework provides no specific standards regarding mandatory token distribution disclosures, governance concentration limits, or statutory liability for misleading decentralization claims. This regulatory gap leaves retail investors vulnerable to predatory rug pulls and governance capture, showing that an entity-based regulatory framework is fundamentally blind to off-chain and on-chain governance manipulation (Sun et al., 2024).

Benchmarking the national regulatory trajectory against international standards highlights the need to accelerate modernization. The Financial Action Task Force mandates that virtual asset service providers strictly implement the Travel Rule to combat illicit financial flows and enhance institutional transparency. While domestic regulations set foundational anti-money laundering obligations for centralized exchanges, cross-exchange data-sharing mechanisms remain technically fragmented. The Financial Stability Board emphasizes the principle of identical regulation for identical activities and risks as a global baseline for crypto asset oversight. Aligning domestic policies with this principle requires supervisory authorities to extend their regulatory perimeter beyond formal corporate licensing to encompass the actual economic functions performed by digital intermediaries, ensuring that decentralized interfaces follow proportionate accountability standards.

The International Organization of Securities Commissions explicitly warns against the regulatory illusion of absolute decentralization within digital asset markets. Their latest policy recommendations urge national regulators to identify the responsible persons exercising factual control over decentralized financial protocols, targeting governance token concentration and administrative key holders. Integrating this approach into the national framework would directly address the normative gaps identified within the DeFi-Social quadrant, allowing authorities to pierce the veil of pseudo-decentralization. The Organization for Economic Co-operation and Development similarly advocates for robust consumer protection frameworks that mandate clear technical risk disclosures and standardized smart contract audits before public deployment. Incorporating these international benchmarks into upcoming financial regulations will shift the national digital asset regime from a reactive compliance model to a proactive, risk-calibrated ecosystem.

Effectively safeguarding retail crypto asset investors in Indonesia requires a fundamental paradigm shift from traditional entity-based legal regulation to an activity-based and risk-proportionate regulatory framework. Adopting the "same activity, same risk, same regulatory outcome" principle allows regulatory oversight to focus on the economic substance and factual mechanics of financial services rather than structural marketing claims (Barbereau et al., 2023). To realize this regulatory evolution, future policy reforms under the Financial Services Authority must prioritize targeted reconstructive pillars. First, statutory accountability standards must be established for perimeter actors that factually facilitate investor access or exercise operational control over digital asset services. Codifying a legal duty of care and technical disclosure obligations for commercial front-end providers and fiat gateways ensures protection at the crucial interface where off-chain intent meets on-chain execution. Second, regulatory frameworks must enforce rigorous standardized

disclosure obligations regarding tokenomics design, smart contract audit reports, and insider affiliations to reduce information asymmetries (Aquilina et al., 2024).

Digital market surveillance capabilities must be modernized and expanded beyond traditional exchange order books to encompass cross-platform promotional activities, social media coordination, and automated trading algorithms. Regulators require advanced digital forensic tools to detect and sanction wash trading, insider listing abuses, and influencer-led manipulative schemes across fragmented digital channels. Legal recovery and remedial mechanisms must be modernized simultaneously to provide meaningful redress for retail losses occurring in both centralized and decentralized environments. This modernization entails establishing statutory investor compensation funds financed by platform licensing fees, clarifying cross-border asset recovery procedures, and introducing collective redress mechanisms that enable retail investors to seek joint remedies following systemic breaches. The Two-Dimensional Fraud Matrix provides supervisory authorities with the necessary conceptual taxonomy to implement this differentiated regulatory strategy, ensuring interventions are calibrated to the precise risk characteristics and practical distribution of accountability within the crypto asset ecosystem.

CONCLUSION

The structural heterogeneity of crypto services and distinct operational fraud vectors produce fundamentally different categories of legal risk that impact retail investors. The Two-Dimensional Fraud Matrix establishes a multidimensional taxonomy that identifies four primary fraud configurations across the centralized-decentralized spectrum. Each quadrant is characterized by unique patterns of direct asset loss, cognitive information distortion, and procedural barriers to legal recovery. The normative evaluation reveals a critical asymmetry within national digital financial asset regulations following the enactment of Law Number 4 of 2023. While the positive legal framework provides relatively comprehensive protection for risks concentrated within centralized environments through traditional administrative licensing and governance obligations, current statutory norms remain fundamentally ill-equipped to address risks arising from decentralized structures involving smart contract vulnerabilities, deceptive tokenomics, and governance capture.

Resolving this empirical-normative divide requires the legal protection framework to evolve from a rigid, entity-based model to an integrated penal policy and risk-proportionate regulatory paradigm. Because decentralized fraud schemes operate through automated code and pseudonymous networks, regulatory and law enforcement mechanisms must expand beyond formal institutional status to target the natural or legal persons behind the digital ecosystem. Realizing this transition requires rigorous application of material and formal criminal law instruments, including electronic-based fraud provisions under the Electronic Information and

Transactions Law, financial-sector criminal sanctions under the Financial Sector Development and Strengthening Law, and commercial fraud rules under the New Criminal Code.

By grounding enforcement in demonstrable criminal intent and adhering to the *ultima ratio* principle, the legal system can prosecute core developers and insider cartels who deploy exploitative mechanisms while safeguarding legitimate technological innovation. By synthesizing empirical fraud typologies with robust penal accountability, policymakers gain a comprehensive baseline for designing responsive legal mechanisms. This reconstructive foundation ensures that future statutory reforms successfully balance digital financial innovation with substantive penal protection and unhindered access to justice for retail investors.

ACKNOWLEDGMENTS

The authors express their sincere gratitude to Indonesian Christian University and Warith Al-Anbiyah University for their institutional and academic support throughout the conduct of this research. Special appreciation is extended to the legal scholars, regulatory experts, and digital forensics practitioners who provided valuable insights into crypto asset governance and financial sector regulation. The authors also wish to thank the editorial board and anonymous reviewers of *Justitia Jurnal Hukum* for their constructive evaluations and insightful recommendations, which significantly refined the quality of this manuscript.

REFERENCES

Aquilina, M., Frost, J., & Schrimpf, A. (2024). Decentralized finance (DeFi): a functional approach. *Journal of Financial Regulation*, *10*(1), 1–27.

Ardia, D., & Bluteau, K. (2024). Twitter and cryptocurrency pump-and-dumps. *International Review of Financial Analysis*, *95*, 103479.

Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, *73*, 102251.

Barczentewicz, M., & de Gândara Gomes, A. (2024). Crypto-asset market abuse under EU MiCA. *European Journal of Risk Regulation*, 1–18.

Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi crime landscape: An evidence-based picture. *Journal of Cybersecurity*, *11*(1), tyae029.

Charamba, K., Shum, Y. Y. J., & Arner, D. W. (2025). Building Castles in the Sky?: The Myth of Decentralized Finance and the Necessity of Legal Ordering. *Wash. U. Global Stud. L. Rev.*, *25*, 1.

Chen, Y.-L., Chang, Y. T., & Yang, J. J. (2023). Cryptocurrency hacking incidents and

the price dynamics of Bitcoin spot and futures. *Finance Research Letters*, *55*, 103955.

Cheraghali, H., Molnár, P., Storsveen, M., & Veliqi, F. (2024). The impact of cryptocurrency-related cyberattacks on return, volatility, and trading volume of cryptocurrencies and traditional financial assets. *International Review of Financial Analysis*, *95*, 103439.

Costello, A., & Gundur, R. V. (2026). Decoding Crypto Asset Fraud: A Crime Script Analysis of Crypto Ponzi, Rug Pull, and Mint-and-Run Schemes. *Journal of Economic Criminology*, 100239.

Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: digital assets and space transition. *Journal of Financial Crime*, *30*(1), 205–220.

Efendi, J. (2022). *Metode Penelitian Hukum Normatif dan Empiris Edisi Kedua*. Prenada Media.

Grobys, K., Dufitinema, J., Sapkota, N., & Kolari, J. W. (2022). What's the expected loss when Bitcoin is under cyberattack? A fractal process analysis. *Journal of International Financial Markets, Institutions and Money*, *77*, 101534.

Jaffri, A. M. (2026). Regulating crypto assets in the United States: balancing regulatory effectiveness, investor protection, and cross-border challenges. *Capital Markets Law Journal*, *21*(2), kmag015.

John, K., Kogan, L., & Saleh, F. (2023). Smart contracts and decentralized finance. *Annual Review of Financial Economics*, *15*(1), 523–542.

Kalacheva, A., Kuznetsov, P., Vodolazov, I., & Yanovich, Y. (2026). Detecting rug pulls in decentralized exchanges: The rise of meme coins. *Blockchain: Research and Applications*, *7*(2), 100336.

Ledoux, E. L., & Smaili, N. (2025). Cryptocurrency frauds: the FTX story. *Journal of Financial Crime*, *32*(3), 530–544.

Li, N., Qi, M., Xu, Z., Zhu, X., Zhou, W., Wen, S., & Xiang, Y. (2025). Blockchain cross-chain bridge security: Challenges, solutions, and future outlook. *Distributed Ledger Technologies: Research and Practice*, *4*(1), 1–34.

Marzuki, P. M. (2019). *Penelitian Hukum* (Cetakan Ke). Kencana.

Milunovich, G., & Lee, S. A. (2022). Measuring the impact of digital exchange cyberattacks on Bitcoin Returns. *Economics Letters*, *221*, 110893.

Nghiem, H., Muric, G., Morstatter, F., & Ferrara, E. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*, *182*, 115284.

Salami, I. (2021). *Challenges and approaches to regulating decentralized finance*.

Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, *10*(2), 213–242.

Srifa, S., Yanovich, Y., Vasilyev, R., Rupasinghe, T., & Amelin, V. (2025). Rug pull detection on decentralized exchange using transaction data. *Blockchain: Research and Applications*, 100275.

Sun, X., Stasinakis, C., & Sermpinis, G. (2024). Decentralization illusion in Decentralized Finance: Evidence from tokenized voting in MakerDAO polls. *Journal of Financial Stability*, *73*, 101286.

Trozze, A., Davies, T., & Kleinberg, B. (2023). Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering. *Forensic Science International: Digital Investigation*, *46*, 301575.

Trozze, A., Kleinberg, B., & Davies, T. (2024). Detecting DeFi securities violations from token smart contract code. *Financial Innovation*, *10*(1), 1–35.

Van Der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, *9*(1), 22.

Wang, Y. (2024). Do cryptocurrency investors in the UK need more protection? *Journal of Financial Regulation and Compliance*, *32*(2), 230–249.

Widiarty, W. S. (2024). *Buku Ajar Metode Penelitian Hukum*. Publika Global Media.

Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: new challenges for compliance. *Journal of Financial Crime*, *30*(1), 97–113.

Wronka, C. (2024). Crypto-asset regulatory landscape: a comparative analysis of the crypto-asset regulation in the UK and Germany: C. Wronka. *Journal of Asset Management*, *25*(4), 417–426.