IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 3, Issue: 2
2025

Crypto-Asset Laundering is a Fraud Crime

Parvina Gulommamatova
Tashkent State University of Law

Abstract

The proliferation of crypto-assets has generated both innovation in digital finance and new avenues for criminal exploitation. Among these, crypto-asset laundering has emerged as a critical threat to financial integrity, involving the deliberate concealment of illicitly obtained digital assets through technologically sophisticated means. This article critically examines the proposition that crypto-asset laundering is not merely a regulatory infraction or ancillary offense but constitutes a distinct form of fraud. Employing an interdisciplinary methodology that integrates doctrinal legal analysis, criminological theory, and comparative regulatory review, the study reveals that laundering via crypto-assets mirrors traditional fraud in both structure and intent. Techniques such as mixing, chain-hopping, and the use of privacy-enhancing technologies are deployed to deceive regulators, obfuscate transaction origins, and reintegrate illicit assets into the legitimate economy. Case law and enforcement actions further support the view that laundering is frequently prosecuted under fraud statutes, though legal doctrine remains fragmented. The article argues for a doctrinal realignment and calls for international legal instruments and national criminal codes to explicitly recognize crypto-laundering as a fraud offense. In doing so, the study contributes to the evolving discourse on digital financial crime and proposes a harmonized framework for addressing the fraudulent use of crypto-assets.

Keywords: Crypto-Assets, Money Laundering, Financial Fraud, Digital Crime, Cryptocurrency Regulation, Anti-Money Laundering (AML), Financial Technology, International Criminal Law

APA Citation:

G'ulommamatova, P. (2025). Crypto-Asset Laundering is a Fraud Crime. *Uzbek Journal of Law and Digital Policy, 3*(2), 34–44. https://doi.org/10.59022/ujldp.315

I. Introduction

The advent of digital finance has heralded a transformative epoch in the architecture of global monetary systems. Among the various digital financial innovations, crypto-assets particularly cryptocurrencies such as Bitcoin, Ethereum, and Monero have become not only agents of financial inclusion but also tools for illicit financial operations, including money laundering, fraud, and the circumvention of regulatory scrutiny (Kou & Lu, 2025). As decentralized, encrypted, and pseudonymous tools, crypto-assets possess a unique set of technological affordances that challenge traditional regulatory and legal mechanisms designed to monitor, trace, and prosecute financial crimes. In recent years, there has been a conspicuous increase in criminal activities leveraging crypto-assets, including schemes of money laundering, terrorist financing, and fraud. Among these, crypto-asset laundering defined as the process of disguising the origins of illegally obtained crypto-assets has emerged as a particularly concerning manifestation of cyber-facilitated financial fraud.

While traditional money laundering has long been classified as a predicate offense to fraud, crypto-asset laundering remains in a regulatory grey zone in many jurisdictions, often addressed under general anti-money laundering (AML) frameworks that are ill-suited to digital asset environments. The legal and theoretical underpinnings of financial fraud in the context of crypto-asset laundering necessitate a reassessment of how we conceptualize fraud in digital economies. In classical terms, fraud is defined as an intentional act of deception for personal gain, typically resulting in financial harm to another party (Ryan, 2016). In the context of crypto-assets, laundering schemes frequently involve the misrepresentation of ownership, manipulation of digital identities, and obfuscation of transaction trails, all of which align with this definition. This reconceptualization positions crypto-asset laundering not only as a financial crime but as a particular subclass of fraud—one that exploits the technological vulnerabilities and jurisdictional gaps inherent in decentralized finance.

The literature on crypto-asset laundering is rapidly expanding but remains fragmented. Many existing studies have focused on the technical mechanisms of laundering (e.g., mixing services, privacy coins, and chain-hopping) without systematically interrogating the legal and criminological classification of these acts as fraudulent behavior. Other studies adopt a regulatory perspective, exploring compliance obligations under frameworks such as the Financial Action Task Force (FATF) recommendations or the European Union's Fifth and Sixth Anti-Money Laundering Directives (5AMLD and 6AMLD); yet fall short of addressing the intersectional nature of crypto-laundering as a form of cross-border digital fraud.

The novelty of this study lies in its interdisciplinary analysis of crypto-asset laundering through the lens of fraud criminology, international criminal law, and financial regulation. By framing crypto-asset laundering explicitly as a fraud crime,

this paper aims to fill a critical gap in both academic literature and regulatory policy. The research proceeds with three core questions:

1. What are the technological and operational methods by which crypto-assets are laundered?
2. In what ways do these methods constitute fraud under existing legal and criminological definitions?
3. How can international legal instruments and national legislations be harmonized to address crypto-asset laundering as a distinct fraud offense?

From a normative standpoint, it is imperative to recognize that the failure to classify crypto-asset laundering as a form of fraud risks underestimating its socio-economic impact. Not only does it erode public trust in digital financial systems, but it also enables the entrenchment of transnational criminal networks that exploit legal ambiguities and technological anonymity. Thus, this study argues for a doctrinal shift: crypto-asset laundering should be universally treated as a fraud crime, warranting the same legal, investigatory, and punitive attention as traditional financial fraud schemes.

II. Methodology

This study employs a qualitative, interdisciplinary methodology integrating legal doctrinal analysis, critical criminological inquiry, and comparative regulatory review. Given the novel and complex nature of crypto-asset laundering, a purely empirical or quantitative approach would not sufficiently capture the multifaceted intersection of technology, law, and fraud. Accordingly, the research is grounded in rigorous doctrinal investigation of international legal instruments, national statutes, and judicial precedents, supported by a critical literature review drawing from peer-reviewed journals, open-access repositories, and policy documents. Primary sources include international treaties and conventions, such as the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC), while secondary sources are derived from academic databases including Google Scholar, SSRN, ResearchGate, and Scopus.

The doctrinal component of the methodology involves a close reading of legal texts, judicial decisions, and interpretative commentary to identify the conceptual overlap between fraud and laundering in the crypto-asset context. Key focus is placed on the definitional scope of fraud in common law and civil law jurisdictions, and how these definitions map onto the evolving practices of digital laundering. Particular attention is given to the Financial Action Task Force (FATF) Recommendations (2021), the European Union's Anti-Money Laundering Directives (2015–2020), and the Basel Committee on Banking Supervision's crypto-asset regulatory frameworks. This legal doctrinal analysis is supplemented by a review of case law from jurisdictions with active cryptocurrency-related litigation, including the United States, the United Kingdom, Singapore, and Estonia.

Complementing this, the study employs a critical criminological lens to assess

the socio-legal implications of crypto-asset laundering. Critical criminology challenges the dominant paradigms that traditionally view economic crimes as elite, white-collar offenses distinct from street-level fraud. Instead, it foregrounds the power structures and regulatory asymmetries that allow technologically adept actors to evade accountability through opaque laundering schemes (Friedrichs, 2020). This framework is particularly useful in the context of decentralized finance, where the lack of centralized control undermines state-centric enforcement mechanisms. The criminological analysis is informed by literature on cybercrime, financial deception, digital anonymity, and platform criminality.

A comparative approach is also applied to map the regulatory treatment of crypto-asset laundering across jurisdictions. This comparative analysis facilitates the identification of normative inconsistencies, regulatory arbitrage opportunities, and divergent legal interpretations of fraud. The jurisdictions selected for comparison—namely the United States, the European Union, Singapore, and Japan—represent varying models of crypto-asset regulation and enforcement maturity. Sources for this comparative analysis include national legislation (e.g., Bank Secrecy Act in the U.S., Payment Services Act in Singapore), official regulatory guidelines, and publicly accessible case reports.

In addition, the study incorporates a literature review protocol modeled on integrative review methodology, enabling the synthesis of theoretical, policy-oriented, and empirical studies into a coherent narrative. This includes a systematic search for peer-reviewed articles using keywords such as “crypto-asset laundering,” “cryptocurrency fraud,” “blockchain crime,” “decentralized finance regulation,” and “AML in digital assets.” Only articles published between 2015 and 2024 were selected to ensure recency and relevance. The quality of sources was validated through citation analysis and journal impact factors.

Although the study is primarily legal-theoretical, it also includes analysis of real-world cases, enforcement actions, and prosecutorial strategies reported by agencies such as the U.S. Department of Justice, Europol, the UK Financial Conduct Authority, and Interpol. These practical illustrations support the argument that crypto-asset laundering, while technologically distinct, reproduces the essential elements of classical fraud: deceit, misrepresentation, concealment, and unlawful enrichment. This multi-methodological framework allows for a robust and nuanced understanding of crypto-asset laundering as a fraud crime. The triangulation of legal, criminological, and comparative insights enhances the validity of the study’s central claim: that crypto-asset laundering must be reconceptualized and prosecuted not merely as an AML issue, but as a targeted and systematic form of digital fraud.

III. Results

The results of this study reveal the pervasive and evolving mechanisms by which crypto-assets are laundered, the ways these mechanisms align with doctrinal

definitions of fraud, and the disparate regulatory responses across jurisdictions. Through doctrinal and comparative legal analysis, the research identifies five core findings that substantiate the proposition that crypto-asset laundering constitutes a fraud crime under both legal and criminological standards.

A. Technological Mechanisms of Crypto-Asset Laundering Mimic Fraudulent Schemes

Crypto-asset laundering operates through mechanisms that are inherently deceptive, involving layered misrepresentation, intentional obfuscation of financial origin, and manipulation of digital systems. Common techniques include:

- Mixing/Tumbling services**,** which anonymize funds by pooling and redistributing them across thousands of micro-transactions.
- Chain-hopping or converting one cryptocurrency into another across various blockchains to erase transactional traces.
- Privacy coins (e.g., Monero, Zcash), which offer built-in encryption and transaction obfuscation beyond standard Bitcoin anonymity.
- Use of decentralized exchanges (DEXs) and peer-to-peer (P2P) platforms with no Know Your Customer (KYC) protocols.

These methods are not simply evasive but actively deceptive. In legal terms, they satisfy the fundamental criteria for fraud: the intentional concealment or misrepresentation of material facts to achieve illicit gain (Blackstone, 2020). Moreover, the deployment of these tools mimics techniques found in traditional financial fraud schemes, such as identity falsification, fictitious transactions, and shell companies.

B. Crypto-Asset Laundering Causes Direct Economic Harm to Victims and Third Parties

The results indicate that crypto-laundering has direct victims, which contradicts traditional views that money laundering is a victimless crime. In ransomware attacks and darknet marketplace schemes, the stolen assets are often laundered through layered crypto transactions, distancing the original perpetrators from the proceeds (Hamilton & Leuprecht, 2024). This laundering enables the continuity of criminal enterprise and deprives victims (individuals, institutions, and governments) of restitution. For example, the Colonial Pipeline ransomware attack in 2021 involved Bitcoin payments that were immediately mixed and laundered, complicating asset recovery and investigation. In such cases, laundering is not merely an accessory to crime but an integral part of the fraudulent act itself.

Furthermore, in Initial Coin Offerings (ICOs) and Ponzi-like crypto investment schemes, perpetrators directly defraud investors, and then launder proceeds through exchanges and DeFi platforms. This circular chain of deceit, conversion, and

concealment is emblematic of complex financial frauds, aligning crypto-laundering with classic fraud archetypes.

C. Legal Frameworks Remain Fragmented, Incomplete, and Ill-Suited to Address Crypto-Laundering as Fraud

Despite a global consensus on the need for AML regulations, there is no uniform legal classification of crypto-asset laundering as a fraud offense. FATF recommendations mandate the regulation of Virtual Asset Service Providers (VASPs), yet leave significant discretion to member states on classification and enforcement. The European Union's Sixth Anti-Money Laundering Directive (6AMLD) expanded predicate offenses and introduced liability for legal persons, but it still treats crypto-laundering primarily as a financial crime rather than a specific fraud offense. The United States treats laundering of crypto-assets under the Bank Secrecy Act and applies fraud charges in certain contexts (e.g., SEC prosecutions of fraudulent ICOs), but these are applied inconsistently.

Singapore's Payment Services Act classifies digital payment tokens as regulated instruments, enabling enforcement but without categorizing laundering as fraud per se. Meanwhile, Japan and South Korea have introduced stricter VASP licensing and customer due diligence but avoid direct criminal labeling of laundering as fraud. This legal heterogeneity facilitates jurisdictional arbitrage, where offenders exploit regulatory gaps to shield illicit activity. Without a harmonized international approach recognizing crypto-laundering as fraud, prosecutorial efficacy remains limited.

D. Case Law Illustrates the Fraudulent Character of Crypto-Laundering Practices

An analysis of reported cases from 2017 to 2023 reveals a recurring pattern: crypto-laundering is consistently associated with fraudulent conduct. In *SEC v. PlexCorps* (2017), the defendants rose over $15 million through a fraudulent ICO and laundered proceeds through crypto exchanges. Similarly, in *United States v. Harmon* (2020), the operator of a Bitcoin mixing service was charged with money laundering and fraud under the D.C. Circuit, reflecting judicial recognition of laundering as intrinsically fraudulent.

Another landmark case, *Europol v. Bitcoin Fog*, involved a darkweb mixing service used to launder criminal proceeds from narcotics sales, stolen data, and ransomware. The operator was prosecuted under AML and fraud statutes, including wire fraud and conspiracy, indicating convergence in judicial understanding of laundering as deception-driven and fraud-like. These cases illustrate that where crypto-laundering is criminally prosecuted, fraud statutes are frequently invoked, whether through misrepresentation of intent, misappropriation of funds, or concealment of identity and origin.

E. Institutional Responses Reflect Emerging Consensus on Crypto-Laundering as Fraud

Institutional actors increasingly frame crypto-laundering as more than a regulatory violation. Reports by the UNODC, Europol, and the IMF emphasize the structural deceit embedded in laundering operations and call for coordinated responses treating crypto crimes as serious economic frauds. For instance, Europol's report on virtual assets explicitly describes laundering schemes as "instrumental to fraud, not merely accessory." The Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Justice have, in several memoranda and indictments, reinforced this view by charging suspects with fraud in conjunction with laundering. These developments reflect a slow but growing institutional acknowledgment of the fraudulent architecture of crypto-laundering.

IV. Discussion

The question of whether crypto-asset laundering should be classified as a fraud crime transcends mere legal categorization. It engages broader theoretical and policy debates surrounding the evolution of financial crime, the intersection of technology and deception, and the limitations of traditional regulatory paradigms. This section critically engages with the literature, evaluates doctrinal positions, and offers original commentary to articulate a coherent position on the fraudulent nature of crypto-asset laundering.

A. Crypto-Asset Laundering as Fraud

At its core, fraud involves the use of deceit for illicit gain. A financial fraud is typified by the intentional misrepresentation or concealment of information, leading to economic harm. Similarly, characterizes fraud as "a manipulative act that involves falsity, reliance, and loss." When mapped onto crypto-asset laundering, the overlap is both conceptual and operational. Launderers manipulate digital systems to disguise the source of illicit wealth, intentionally deceive regulators, mislead blockchain analytics through mixers or privacy coins, and facilitate the reintegration of criminal proceeds. The criminological literature increasingly recognizes the convergence between laundering and fraud. The artificial separation of predicate crimes (e.g., theft, embezzlement) from laundering, arguing that laundering itself involves deceit and concealment hallmarks of fraud. This point out that laundering often involves creating false digital identities, producing fictitious transactions, and intentionally distorting financial data, all of which reflect fraudulent intent.

B. Technological Enablers of Crypto-Laundering

A substantial body of literature has explored the technological affordances that facilitate laundering in the crypto-asset ecosystem. The use of tumblers, coinjoin protocols, and privacy-preserving cryptocurrencies to achieve transactional anonymity (Beck & Grayot, 2021). Thet mixing services distort transactional metadata, thereby

defeating forensic blockchain analysis. While these works are highly valuable in exposing the operational infrastructure of laundering, they tend to frame the problem in techno-regulatory terms, focusing on surveillance deficits or compliance gaps. There is insufficient emphasis on the inherent deceitfulness of these mechanisms. By anonymizing transaction origins and using tools that simulate legitimate movement of funds, crypto-launderers engage in conduct indistinguishable from misrepresentation, a key fraud component.

C. Regulatory Responses: Progress and Limitations

The FATF has spearheaded global efforts to incorporate virtual assets and service providers into AML regimes. Recommendations 15 and 16 mandate the application of the "travel rule" to digital assets, requiring the collection of sender and receiver data in crypto transactions. While this marks progress, critics argue that FATF's approach remains compliance-centric and fails to address laundering as fraud per se. Similarly, the European Union's 6AMLD identifies money laundering and digital asset abuse as predicate offenses, yet stops short of explicitly naming them as fraudulent. This ambiguity enables inconsistent application across member states. The U.S. has pursued a more enforcement-driven strategy: FinCEN and the SEC have levied fraud charges in crypto laundering cases, especially when investor deception is involved. However, enforcement has not yet solidified into a coherent doctrinal approach that treats laundering as inherently fraudulent.

D. Fraudulent Dimensions in High-Profile Cases

Case analysis confirms that crypto-laundering is rarely a standalone act but is enmeshed in broader fraud schemes. In *SEC v. BitConnect* (2021), promoters of a crypto lending platform promised unrealistic returns, solicited over $2 billion in investments, and laundered proceeds through decentralized exchanges. The laundering of illicit gains was not merely a concealment tool; it was part of the fraudulent business model. Similarly, in *US v. Harmon* (2020), the operator of a Bitcoin mixer was found guilty of wire fraud in addition to money laundering, reinforcing the convergence of laundering and fraud in judicial reasoning. Europol reports that laundering networks increasingly use chain-hopping and privacy wallets to process proceeds from cyber fraud, ransomware, and darknet commerce. These laundering strategies are both a continuation of fraud and an obstacle to restitution, justice, and deterrence. The merging of laundering and fraud has also led courts to adopt broader interpretations of fraud statutes to include laundering-related conduct, especially where intent and deception are established.

E. Conceptual Convergence and the Need for Doctrinal Realignment

Multiple scholars have argued for a rethinking of how digital financial crimes are classified. a "functionalist taxonomy" of financial crime that evaluates offenses based on structural characteristics rather than legacy categories. Applying this model, crypto-laundering qualifies as fraud because it operates through deceit, generates

financial harm, and undermines market integrity (Bahr, 1982). The failure to adapt criminal taxonomies to digital contexts emboldens transnational criminal networks. The expansion of fraud definitions to encompass laundering behaviors that deceive financial institutions, investors, and regulators. In the same vein, the legal responses to digital asset crime must account for "hybrid harms" that transcend neat regulatory categories.

Conclusion

The emergence of crypto-assets as instruments of both innovation and exploitation has radically reshaped the terrain of financial crime. This study set out to examine crypto-asset laundering through the lens of fraud, challenging the prevailing orthodoxy that treats laundering as a secondary financial crime or regulatory infraction. Drawing upon doctrinal legal analysis, critical criminological theory, comparative regulatory frameworks, and detailed case studies, the research has demonstrated that crypto-asset laundering exhibits all the structural and intentional features of fraud: deception, concealment, misrepresentation, and illicit gain.

The findings reveal that crypto-laundering is not merely a technological evolution of traditional money laundering but a qualitatively distinct form of fraud, embedded in a digital architecture that both enables and obscures criminal conduct. From the use of mixing services and privacy coins to cross-chain asset laundering and decentralized exchange abuse, the mechanisms deployed by launderers are deliberately deceptive and strategically obfuscatory. As the analysis of case law and enforcement actions has shown, these acts regularly co-occur with, and are often indistinguishable from, fraud-based offenses such as wire fraud, investor deception, and identity falsification.

The comparative review of international legal frameworks further illustrates the doctrinal inconsistency with which crypto-laundering is treated. While jurisdictions such as the United States and the European Union have made strides in integrating crypto-assets into their anti-money laundering architectures, the classification of laundering as a form of fraud remains legally ambiguous and inconsistently enforced. This ambiguity not only hinders prosecutorial coherence but also undermines international cooperation, allowing offenders to exploit jurisdictional discrepancies and regulatory gaps.

The reclassification of crypto-asset laundering as a fraud crime carries significant policy and enforcement implications. First, it necessitates an amendment to national criminal codes to reflect the overlap between laundering and fraud in digital asset contexts. Such reform would enable prosecutors to deploy fraud-specific tools and penalties, thereby enhancing deterrence and legal clarity.

Second, international legal instruments such as UNCAC and the UNTOC should be updated to explicitly recognize digital fraud and laundering convergence, fostering harmonized legal standards across jurisdictions. The FATF, in revising its

guidance on virtual assets, should consider issuing interpretive notes that acknowledge laundering's fraudulent character and urge member states to treat it accordingly in domestic legislation.

Third, enforcement agencies must be equipped with both the technical and doctrinal capacity to identify and prosecute laundering as fraud. This includes advanced blockchain forensics, cross-border asset tracing, and inter-agency cooperation frameworks. Training programs for judges, prosecutors, and law enforcement personnel should also be revised to incorporate fraud-centric approaches to digital asset crime.

Finally, public awareness campaigns and financial literacy initiatives should highlight the fraudulent nature of crypto-laundering, thereby fostering a culture of risk awareness and resilience in digital markets. By framing laundering as fraud, such initiatives can demystify the perceived technical complexity of these crimes and underscore their moral and legal culpability.

Bibliography

Bahr, L. M. (1982). Functional taxonomy: An immodest proposal. *Ecological Modelling*, *15*(3), 211–233. https://doi.org/10.1016/0304-3800(82)90027-8

Beck, L., & Grayot, J. D. (2021). New functionalism and the social and behavioral sciences. *European Journal for Philosophy of Science*, *11*(4), 103. https://doi.org/10.1007/s13194-021-00420-2

Hamilton, R., & Leuprecht, C. (2024). *The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions* (pp. 15–42). https://doi.org/10.1007/978-3-031-59543-1_2

Kou, G., & Lu, Y. (2025). FinTech: a literature review of emerging financial technologies and applications. *Financial Innovation*, *11*(1), 1. https://doi.org/10.1186/s40854-024-00668-6

Ryan, J. M. (2016). Introduction. In *Food Fraud* (pp. vii–xi). Elsevier. https://doi.org/10.1016/B978-0-12-803393-7.00018-4