IJCCL

Journal of Civil Criminal Law

E-ISSN: 3089-6878
P-ISSN: 3089-6886

Research Article

Reconstructing Criminal Asset Recovery in Indonesia's Digital Financial Crime: Integrating Criminal Liability, Digital Asset Tracing, and FATF Standards

Muhammad Ridwan lubis[1]*, Rini Novita[2], Diana Lubis[3]

[1] Hukum, Ilmu Hukum, Universitas Muslim Nusantara Al Wasliyah, Medan, Sumut, Indonesia; e-mail: muhammadridwanlubis76@gmail.com
[2] Hukum, Ilmu Hukum, Unversitas Darma Agung, Medan, Sumut, Indonesia; e-mail: rininovita202@gmail.com
[3] Hukum, Ilmu Hukum, Unversitas Darma Agung, Medan, Sumut, Indonesia; e-mail: dianabeby147@gmail.com
* Corresponding Author: Muhammad Ridwan lubis

Abstract: The rapid expansion of the digital economy, financial technology, cryptocurrencies, virtual assets, and blockchain has transformed financial transactions while simultaneously creating new opportunities for digital financial crime. Crimes such as online fraud, crypto-enabled money laundering, ransomware attacks, and cross-border illicit financial flows increasingly exploit technological innovations, making criminal asset recovery more complex. These developments expose significant weaknesses in Indonesia's legal framework, particularly regarding the regulation of digital assets, tracing of criminal proceeds, and enforcement of effective recovery mechanisms. This study examines the shortcomings of Indonesia's criminal asset recovery regime by analyzing the interaction between criminal liability, digital asset tracing, and compliance with Financial Action Task Force (FATF) standards. The research employs a doctrinal legal method using statutory, conceptual, comparative, case, and law reform approaches. The findings reveal that Indonesia's regulatory framework remains fragmented and inadequately addresses the unique characteristics of cryptocurrencies and virtual assets. Regulatory inconsistencies, limited blockchain investigative capacity, weak beneficial ownership verification, fragmented institutional coordination, and incomplete alignment with FATF standards reduce the effectiveness of criminal asset recovery. Accordingly, this study proposes the Integrated Digital Asset Recovery Framework (IDARF), integrating criminal liability, blockchain-based asset tracing, beneficial ownership verification, FATF compliance, international cooperation, due process, human rights protection, and victim-oriented asset recovery. The proposed framework provides a normative foundation for legal reform through the enactment of a Digital Asset Recovery Act, the establishment of a Digital Asset Recovery Center, and strengthened institutional integration to improve Indonesia's capacity to combat digital financial crime.

Keywords: Asset Recovery; Blockchain Analytics; Criminal Liability; Digital Asset Tracing; Digital Financial Crime.

Received: February 16, 2026
Revised: April 10, 2026
Accepted: June 25, 2026
Published: July 27, 2026
Curr. Ver.: July 27, 2026

1. Introduction

The digital transformation of the global economy has fundamentally reconfigured the international financial system through the widespread adoption of digital technologies in commerce, investment, and financial services. Advances in financial technology (fintech), distributed ledger technology (DLT), blockchain, cryptocurrency, virtual assets, central bank digital currencies (CBDCs), and digital payment systems have significantly enhanced the efficiency of cross-border transactions while simultaneously creating increasingly sophisticated forms of financial crime. The speed, cross-border nature, and reduced reliance on conventional financial intermediaries have reshaped law enforcement approaches to evidentiary processes, asset tracing, and the recovery of criminal proceeds. Consequently, the principal challenge for law enforcement authorities is no longer confined to establishing criminal liability but extends to the State's capacity to identify, freeze, seize, confiscate, and recover assets dispersed across digital platforms and blockchain networks (Financial Action Task Force [FATF], 2023; United Nations Office on Drugs and Crime [UNODC], 2023).

This transformation has also generated a regulatory paradox. On the one hand, digitalisation promotes financial inclusion, accelerates commercial transactions, and stimulates the expansion of the digital economy. On the other hand, technological characteristics—including decentralisation, pseudonymity, smart contracts, mixing services, privacy coins, cross-chain bridges, and decentralised finance (DeFi)—provide opportunities for criminal actors to conceal their identities and rapidly transfer illicit proceeds across multiple jurisdictions. According to the FATF (2024), virtual assets are no longer used solely as investment instruments but have become integral to money laundering, terrorist financing, ransomware attacks, digital investment fraud, asset misappropriation, and other forms of cyber-enabled financial crime. These developments demonstrate that digital transformation has altered not only the methods of financial crime but also the nature of criminal proceeds, which are increasingly digital, highly liquid, and capable of being transferred almost instantaneously.

The urgency of these challenges is reflected in recent international reports. The UNODC (2023) estimates that global money laundering accounts for approximately 2–5% of the world's gross domestic product (GDP), equivalent to between USD 800 billion and USD 2 trillion annually, with an increasing reliance on digital financial instruments and virtual assets. Chainalysis (2024) similarly reports that cryptocurrency transactions associated with illicit activities continue to amount to billions of US dollars each year despite the strengthening of regulatory oversight. Europol (2023) has identified a growing use of virtual assets in investment fraud, business email compromise, ransomware, illicit trade conducted through the dark web, and cross-border money laundering. Likewise, INTERPOL (2024) observes that transnational organised criminal groups increasingly exploit blockchain technology, digital asset exchanges, and non-custodial crypto wallets to obscure financial flows, thereby complicating criminal investigations and asset recovery efforts. Accordingly, asset recovery should no longer be regarded merely as the concluding stage of criminal proceedings but rather as a strategic mechanism for depriving offenders of the financial benefits that motivate digital financial crime.

From an economic perspective, digital financial crime extends beyond losses suffered by individual victims and poses substantial risks to the stability of the financial system as a whole. The International Monetary Fund (IMF, 2024) and the World Bank (2023) emphasise that digital financial crime undermines confidence in digital innovation, increases compliance costs within the financial sector, and heightens systemic risks to market integrity. Consequently, the effectiveness of anti-money laundering and counter-terrorist financing (AML/CFT) regimes is no longer assessed solely by the number of offenders prosecuted but also by a jurisdiction's ability to trace, seize, confiscate, and recover criminal assets in a timely, transparent, and accountable manner. This approach is consistent with the FATF framework, which identifies asset recovery as a core indicator of AML/CFT effectiveness under Immediate Outcome 8, together with its recommendations concerning asset tracing, freezing, seizure, and confiscation.

Indonesia faces similar challenges amid its rapidly expanding digital economy. The growth of internet users, the proliferation of e-commerce, the widespread adoption of digital payment systems, the increasing use of blockchain technology, and the expansion of cryptocurrency trading have positioned Indonesia as one of Southeast Asia's largest digital economies. Bank Indonesia (2024) reports that digital payment transactions, including those conducted through the Quick Response Code Indonesian Standard (QRIS), continue to increase annually. Likewise, the Financial Services Authority (*Otoritas Jasa Keuangan*—OJK) has recorded significant growth in technology-based investment activities, enabling broader public access to digital financial services. While these developments contribute to economic growth, they simultaneously expand opportunities for the misuse of digital technologies to facilitate financial crime.

The rapid growth of the digital economy has been accompanied by an escalation in technology-enabled financial offences. Digital investment fraud, online fraud, phishing, identity theft, the misuse of bank accounts as money mules, online gambling, illicit cryptocurrency transactions, and money laundering through digital platforms have become increasingly sophisticated. Annual reports issued by Indonesia's Financial Transaction Reports and Analysis Centre (*Pusat Pelaporan dan Analisis Transaksi Keuangan*—PPATK) indicate a significant rise in suspicious transactions linked to online gambling, electronic fraud, and the use of third-party accounts to disguise the origin of illicit funds. The inherent characteristics of blockchain technology, which enable cross-border asset transfers without reliance on conventional banking systems, further complicate offender identification and asset tracing compared with traditional financial crimes.

These challenges are particularly evident in the proliferation of online gambling, which has emerged as a major law enforcement priority in Indonesia in recent years. Beyond causing substantial economic losses, online gambling is frequently associated with money laundering, nominee account arrangements, the use of digital assets, and transnational criminal networks. Joint enforcement operations undertaken by PPATK, the Indonesian National Police (*Kepolisian Negara Republik Indonesia*), and the Office of the Attorney General of the Republic of Indonesia (*Kejaksaan Republik Indonesia*) have uncovered numerous criminal networks involving thousands of bank accounts, electronic wallets, and digital assets spread across multiple jurisdictions. Nevertheless, the successful dismantling of these networks has not been matched by equivalent success in recovering criminal proceeds, as a substantial proportion of the assets had already been transferred through sophisticated digital mechanisms that remain difficult to trace effectively.

These challenges demonstrate that the principal weakness of Indonesia's law enforcement system lies not in its ability to detect and prosecute criminal offences, but in the effectiveness of recovering criminal proceeds. In practice, the conviction of offenders does not necessarily result in the restitution of state losses or the restoration of victims' rights where assets have been transferred to digital wallets, overseas cryptocurrency exchanges, or blockchain networks characterised by a high degree of anonymity. This reality indicates that a criminal justice system primarily oriented towards punishment is no longer sufficient to address the profit-driven nature of digital financial crime. Accordingly, the effectiveness of law enforcement should be assessed not only by successful prosecutions but also by the State's ability to trace, freeze, seize, confiscate, and recover criminal assets efficiently.

Although Indonesia has enacted a range of legal instruments governing money laundering, cybercrime, personal data protection, and financial sector supervision, their implementation continues to face significant challenges. One of the most pressing issues is the limited capacity to conduct effective asset tracing in relation to digital assets dispersed across blockchain networks and multiple foreign jurisdictions. Unlike conventional assets, which are generally recorded within national administrative systems, digital assets can be transferred through thousands of wallet addresses, decentralised exchanges, and blockchain-based financial protocols without leaving readily verifiable administrative records. Consequently, establishing ownership, identifying the beneficial owner, and demonstrating the nexus between offenders and criminal proceeds have become substantially more complex.

Furthermore, the legal framework governing the seizure and confiscation of digital assets remains fragmented across several statutes. Relevant provisions are dispersed within the Indonesian Code of Criminal Procedure (*Kitab Undang-Undang Hukum Acara Pidana*—KUHAP), Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, and the Personal Data Protection Law. Collectively, these instruments have yet to establish a comprehensive legal regime governing digital assets. This fragmentation creates legal uncertainty regarding the identification, freezing, seizure, management, and enforcement of virtual assets held on blockchain networks or under the control of service providers operating outside Indonesia's jurisdiction. As a result, Indonesia's asset recovery framework has struggled to keep pace with the rapid technological developments increasingly exploited by criminal actors.

These developments underscore a fundamental shift in the objectives of criminal law enforcement from merely detecting and punishing offenders to ensuring the effective recovery of criminal proceeds. Responding to this transformation requires a comprehensive reconstruction of the legal framework that integrates emerging digital technologies, blockchain-based asset tracing mechanisms, and internationally recognised standards governing virtual assets. Without a more adaptive, coherent, and coordinated legal regime, Indonesia's criminal justice system will remain constrained in its ability to deprive offenders of the economic benefits derived from crime, thereby limiting the effective protection of state interests, legal certainty, and the restoration of victims' rights.

2. Literature Review

The complexity of asset recovery in digital financial crime requires an analytical framework that extends beyond conventional criminal law to incorporate technological innovation, international financial governance, and human rights protection. From this perspective, Criminal Liability Theory maintains that criminal responsibility should not be confined to establishing *actus reus* and *mens rea*, but should also ensure the recovery of the economic benefits derived from criminal conduct. This approach is consistent with Asset Recovery Theory, which regards asset tracing, freezing, seizure, confiscation, and restitution as integral components of a modern criminal justice system. Accordingly, the effectiveness of law enforcement should be measured not only by the successful prosecution of offenders but also by the State's capacity to deprive them of the proceeds of crime (Stolen Asset Recovery Initiative [StAR], 2023; FATF, 2023).

This perspective is further reinforced by Deterrence Theory, which argues that criminal sanctions are more effective when they deprive offenders of illicit gains rather than relying solely on imprisonment. In the context of digital financial crime, offenders typically engage in rational cost-benefit calculations, rendering custodial penalties less effective if criminal proceeds can still be concealed through blockchain networks, virtual assets, or cross-border financial transactions. Likewise, Economic Analysis of Law emphasises that an efficient legal system should increase the economic costs of criminal activity through effective seizure and confiscation mechanisms, thereby eliminating the financial incentives for offending (Posner, 2014). This approach is particularly relevant in the digital era, where assets can be transferred rapidly across jurisdictions and are inherently more difficult to trace.

At the same time, technological advancement necessitates a reorientation of legal thinking through the lens of Law and Technology. While blockchain technology has facilitated new forms of financial crime, it has also provided law enforcement authorities with sophisticated investigative tools, including blockchain analytics, distributed ledger forensic analysis, and transaction monitoring. Nevertheless, the use of these technologies must remain consistent with the principles of the Rule of Law, Due Process of Law, and the protection of human rights, ensuring that digital asset tracing and confiscation comply with the requirements of legality, proportionality, accountability, and personal data protection. Within the Indonesian context, this approach aligns with the principles of Progressive Law, which views law as an instrument for responding to social and technological change, and Corrective Justice, which prioritises the restoration of losses suffered by the State and victims. Consequently, the effectiveness of an asset recovery regime should be assessed through an integrated framework encompassing criminal liability, economic efficiency, corrective justice, technological innovation, and sound legal governance.

International scholarship published between 2021 and 2026 likewise demonstrates increasing attention to the relationship between digital assets, money laundering, and asset recovery mechanisms in response to the evolving challenges of law enforcement in the digital economy. The first body of literature focuses on the implementation of the Financial Action Task Force (FATF) standards governing virtual assets and Virtual Asset Service Providers (VASPs). These studies generally conclude that the effectiveness of anti-money laundering and counter-terrorist financing (AML/CFT) regimes increasingly depends on the adoption of a risk-based approach, beneficial ownership verification, implementation of the FATF Travel Rule, and strengthened cross-border cooperation. However, most existing research concentrates on regulatory compliance and international policy harmonisation, while comparatively little attention has been devoted to the effectiveness of digital asset seizure and recovery within domestic criminal justice systems.

A second body of research examines the use of blockchain analytics, digital forensic investigations, artificial intelligence, and blockchain transaction analysis as tools for tracing digital assets. The literature indicates that the transparent nature of blockchain technology can assist law enforcement authorities in identifying transaction patterns, mapping relationships between digital wallets, and dismantling transnational criminal networks. Nevertheless, the effectiveness of these technologies remains constrained by the use of privacy coins, mixers, tumblers, cross-chain bridges, and decentralised finance (DeFi) protocols that obscure the origin and movement of criminal proceeds. As a result, questions concerning ownership attribution, evidentiary standards, and the legal basis for digital asset confiscation remain unresolved.

Another stream of scholarship explores the application of non-conviction-based confiscation, civil forfeiture, and other asset confiscation mechanisms that do not depend upon a criminal conviction as responses to increasingly sophisticated transnational crime. The literature suggests that these mechanisms can substantially improve asset recovery, particularly where offenders have absconded, died, or remain outside the jurisdiction of domestic courts. At the same time, any expansion of confiscation powers must be accompanied by robust safeguards for Due Process of Law, judicial oversight, and the protection of property rights in order to remain consistent with the principles of the Rule of Law and internationally recognised human rights standards. Consequently, the legitimacy of legal procedures is as important as their operational effectiveness.

A further body of research addresses the role of beneficial ownership transparency and international cooperation in cross-border asset recovery. Existing studies demonstrate that identifying the beneficial owner is a prerequisite for effective asset tracing, particularly where offenders employ shell companies, nominee arrangements, trusts, or virtual assets distributed across multiple global platforms. Although the FATF advocates the establishment of accurate and accessible beneficial ownership registries, implementation remains uneven across jurisdictions, thereby limiting the effectiveness of Mutual Legal Assistance (MLA), asset-sharing arrangements, and the recovery of criminal assets across borders.

Taken together, the international literature recognises asset recovery as a key indicator of effective law enforcement against digital financial crime. However, a synthesis of studies published between 2021 and 2026 reveals three significant research gaps. First, most studies examine criminal liability, blockchain technology, and AML/CFT frameworks as separate fields, resulting in the absence of an integrated framework linking criminal law, digital technology, and international financial governance. Secondly, the majority of existing scholarship is based on the experience of common law jurisdictions, requiring further conceptual and normative adaptation before its findings can be effectively applied within civil law systems, including Indonesia. Thirdly, there remains a notable lack of research proposing a comprehensive legal reconstruction that integrates Criminal Liability, Digital Asset Tracing, Beneficial Ownership Verification, and the FATF Recommendations into a unified asset recovery model. These gaps highlight the need for a more integrated legal framework capable of responding to the distinctive characteristics of digital financial crime within Indonesia's legal system.

Research Gap, Novelty

A synthesis of the international literature indicates that research on asset recovery in digital financial crime has expanded considerably in recent years, yet it remains largely fragmented. Most studies focus on strengthening anti-money laundering and counter-terrorist financing (AML/CFT) regimes, regulating virtual assets, applying blockchain analytics in criminal investigations, or adopting non-conviction-based confiscation as an asset recovery mechanism. Although these studies have made valuable contributions to both legal theory and enforcement practice, they have not developed an integrated legal framework that combines criminal liability, digital asset tracing, beneficial ownership governance, and international regulatory standards. Consequently, existing recommendations remain sector-specific and are insufficient to address the increasingly complex, technology-driven, and transnational nature of digital financial crime.

This research gap is particularly evident in Indonesia. Unlike several jurisdictions that have established dedicated legal regimes for the seizure and confiscation of digital assets, Indonesia's regulatory framework remains dispersed across multiple legal instruments, including the Indonesian Code of Criminal Procedure (*Kitab Undang-Undang Hukum Acara Pidana*—KUHAP), Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, the Personal Data Protection Law, and various regulations governing the financial services sector. This fragmented framework has created inconsistencies in the identification, freezing, seizure, management, and recovery of digital assets, particularly where assets are recorded on blockchain networks or managed by service providers operating outside Indonesia's jurisdiction. Accordingly, the challenge extends beyond the inadequacy of substantive legal norms to the absence of an institutional framework capable of integrating criminal liability, digital asset tracing technologies, and international cooperation.

Moreover, previous studies have generally adopted isolated disciplinary perspectives, whether grounded in criminal law, financial regulation, or information technology. Such approaches have been unable to capture the multidimensional nature of digital financial crime, which involves the interaction of blockchain technology, digital identity, beneficial ownership, virtual assets, and the global AML/CFT regime. Effective asset recovery depends not only on proving the commission of a criminal offence but also on the ability of law enforcement authorities to trace digital transactions, identify beneficial owners, strengthen inter-agency coordination, and facilitate cross-border cooperation in accordance with the Financial Action Task Force (FATF) Recommendations. These challenges underscore the need for a legal framework that integrates these interrelated elements into a coherent, adaptive, and technologically responsive model.

Against this background, this study introduces the Integrated Digital Asset Recovery Framework (IDARF) as a novel conceptual model for reconstructing Indonesia's legal framework governing the recovery of criminal assets in digital financial crime. Unlike previous studies, which typically examine asset recovery within the limited context of anti-money laundering regimes or cryptocurrency investigations, IDARF adopts a multidimensional approach that integrates eight interrelated components. These include Criminal Liability as the legal foundation for asset tracing, freezing, seizure, and confiscation; Digital Asset Tracing through electronic transaction analysis and cross-platform financial flow mapping; and the application of Blockchain Analytics to identify relationships among digital wallets, transaction patterns, and illicit financial networks with greater precision.

Furthermore, IDARF strengthens Beneficial Ownership Verification by integrating beneficial ownership records, corporate information, and digital identity systems to address nominee arrangements, shell companies, and layered ownership structures. The framework also harmonises Indonesia's legal regime with the FATF Recommendations, particularly regarding the risk-based approach, supervision of Virtual Asset Service Providers (VASPs), implementation of the FATF Travel Rule, and mechanisms governing asset seizure and confiscation. In addition, the framework reinforces International Cooperation through enhanced Mutual Legal Assistance (MLA), financial intelligence exchange, joint investigation mechanisms, and asset-sharing arrangements designed to address the transnational character of digital financial crime.

As a comprehensive legal framework, IDARF recognises Due Process of Law and the protection of human rights as fundamental principles governing every stage of digital asset tracing, freezing, seizure, and confiscation. This approach ensures that expanded state powers remain consistent with the Rule of Law by safeguarding property rights, promoting procedural transparency, and providing effective judicial oversight. Beyond recovering state losses, the framework seeks to restore victims' rights, strengthen the integrity of the financial system, and eliminate the economic incentives that motivate criminal activity. Accordingly, IDARF extends beyond a purely punitive model by incorporating restorative principles into contemporary criminal justice policy.

This study makes both conceptual and practical contributions. Conceptually, it integrates Criminal Liability Theory, Asset Recovery Theory, Law and Technology, Economic Analysis of Law, and the Rule of Law into a unified analytical framework for digital asset recovery. This integrated perspective broadens the conventional understanding of criminal justice by demonstrating that its effectiveness should be evaluated not only by the successful prosecution of offenders but also by the transparent and accountable recovery of criminal proceeds. From a practical perspective, the study proposes a framework for legal reform that may guide legislators, law enforcement agencies, the Indonesian Financial Transaction Reports and Analysis Centre (*Pusat Pelaporan dan Analisis Transaksi Keuangan*—PPATK), the Financial Services Authority (*Otoritas Jasa Keuangan*—OJK), Bank Indonesia, and other relevant institutions in developing an asset recovery regime that is responsive to technological innovation and aligned with international standards.

Research Objectives

Against this backdrop, the study pursues three principal objectives. First, it critically examines the weaknesses of Indonesia's criminal asset recovery system in addressing digital financial crime, particularly with respect to digital asset tracing, beneficial ownership verification, asset seizure, and cross-border confiscation. Secondly, it evaluates the compatibility of Indonesia's legal framework with international standards, especially the FATF Recommendations, while identifying regulatory areas requiring further harmonisation. Thirdly, it proposes the Integrated Digital Asset Recovery Framework (IDARF) as a legal reconstruction model that is more effective, adaptive, and asset recovery-oriented, while fully respecting Due Process of Law, the protection of human rights, and legal certainty in responding to the evolving challenges of digital financial crime.

The remainder of this article is organised as follows. Following this Introduction, the Methodology section outlines the doctrinal legal research approach supported by conceptual, comparative, and regulatory analysis. The subsequent Discussion examines the structural weaknesses of Indonesia's asset recovery regime and evaluates its compatibility with FATF standards and international practice. The following section develops the proposed Integrated Digital Asset Recovery Framework (IDARF) as a comprehensive model for legal reform. Finally, the article concludes with key findings and policy recommendations intended to support the modernisation of Indonesia's criminal justice system and enhance the effectiveness of asset recovery in addressing digital financial crime.

3. Research Method

This study adopts a doctrinal legal research methodology, focusing on the systematic analysis of legal norms, principles, doctrines, judicial decisions, and national and international legal instruments governing the recovery of criminal assets in digital financial crime. Unlike empirical legal research, which examines the operation of law in practice, doctrinal research seeks to evaluate the coherence, consistency, and adequacy of legal norms through legal interpretation and normative reasoning (Marzuki, 2021; Hutchinson & Duncan, 2012; Van Hoecke, 2011). This approach is appropriate because the principal issues addressed in this study arise from regulatory fragmentation, normative inconsistency, and the inadequacy of Indonesia's legal framework governing the recovery of proceeds derived from digital financial crime. Accordingly, the research aims to identify deficiencies in the existing legal framework, assess its compatibility with international standards, and formulate a legal reconstruction capable of responding to developments in digital financial technology and transnational financial crime.

As a doctrinal study, the analysis conceptualises law as a normative system (*law as it ought to be*), treating legislation, legal doctrine, and general principles of law as its primary objects of inquiry. This approach enables a comprehensive evaluation of the legal framework governing asset tracing, freezing, seizure, confiscation, and the recovery of digital assets, while assessing its consistency with international anti-money laundering and counter-terrorist financing (AML/CFT) standards, the regulation of virtual assets, and beneficial ownership transparency. Consequently, the study goes beyond describing existing legal norms by developing prescriptive legal arguments to support a more adaptive framework for criminal law reform in the era of digital economic transformation.

To achieve these objectives, the research integrates several complementary legal approaches. The statutory approach is employed to examine the structure, substance, and interrelationship of legislation governing criminal asset recovery at both the general and sector-specific levels. The analysis encompasses the Indonesian Criminal Code (Law No. 1 of 2023), the Indonesian Code of Criminal Procedure (*Kitab Undang-Undang Hukum Acara Pidana*—KUHAP), Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, the Personal Data Protection Law, together with implementing regulations issued by the Financial Services Authority (*Otoritas Jasa Keuangan*—OJK), the Financial Transaction Reports and Analysis Centre (*Pusat Pelaporan dan Analisis Transaksi Keuangan*—PPATK), Bank Indonesia, and other relevant institutions. This approach seeks to identify both regulatory harmonisation and normative inconsistencies in addressing the cross-border, decentralised, and blockchain-based characteristics of digital assets.

The study further applies a conceptual approach to examine key legal concepts, including Criminal Liability, Asset Recovery, Digital Asset Tracing, Beneficial Ownership, seizure, confiscation, and the recovery of losses suffered by the State and victims. This approach provides the theoretical foundation for integrating developments in criminal law with emerging digital technologies, allowing these concepts to be analysed as interconnected components of a unified legal framework. It also facilitates a critical assessment of the continued relevance of established legal doctrines in responding to virtual assets, blockchain technology, and financial innovation that remain only partially accommodated within Indonesia's positive law.

A comparative approach is likewise adopted by examining the legal frameworks of jurisdictions that have developed more comprehensive digital asset recovery mechanisms, including the United Kingdom, Singapore, Australia, the United States, Switzerland, and the Member States of the European Union. The comparative analysis focuses on the regulation of virtual assets, implementation of the Financial Action Task Force (FATF) Recommendations, the use of blockchain technology in financial investigations, and mechanisms governing the seizure and confiscation of digital assets. The purpose of this approach is not to transplant foreign legal systems into Indonesia, but rather to identify best practices and legal principles capable of being adapted to Indonesia's civil law tradition. Accordingly, comparative analysis serves both as an evaluative tool and as a normative basis for proposing contextually appropriate legal reforms.

In addition to the statutory approach, the study employs a case approach by analysing both Indonesian and foreign judicial decisions concerning the recovery of criminal proceeds, money laundering, digital asset seizure, and technology-enabled financial crime. Particular attention is given to the ratio decidendi, evolving judicial interpretations of digital assets, and emerging trends in the application of asset recovery principles. Judicial decisions are especially significant because they not only illustrate the practical application of positive law but also demonstrate how courts respond to technological developments that frequently outpace legislative reform.

The research also incorporates a law reform approach as the normative basis for formulating recommendations for legal reconstruction. This approach recognises that legal scholarship should extend beyond explaining the existing law (*ius constitutum*) to proposing the law as it ought to be (*ius constituendum*). Accordingly, the findings derived from statutory, conceptual, comparative, and case analyses are synthesised to formulate recommendations aimed at strengthening digital asset tracing mechanisms, harmonising Indonesia's legal framework with international standards, enhancing cross-border cooperation, and ensuring that asset recovery procedures remain consistent with the principles of Due Process of Law and the protection of human rights.

The study relies on primary, secondary, and tertiary legal materials. Primary legal materials include the Indonesian Criminal Code (Law No. 1 of 2023), the Indonesian Code of Criminal Procedure (KUHAP), Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, the Personal Data Protection Law, together with implementing regulations issued by the Financial Services Authority (OJK), PPATK, Bank Indonesia, and other relevant authorities governing digital assets, electronic transactions, and the financial system. At the international level, the study examines the FATF Recommendations, the FATF Guidance on Virtual Assets and Virtual Asset Service Providers, the United Nations Convention against Corruption (UNCAC), the United Nations Convention against Transnational Organized Crime (Palermo Convention), and other international instruments governing law enforcement cooperation, asset recovery, and anti-money laundering. These primary legal materials are analysed to evaluate the degree of harmonisation between Indonesia's legal framework and international standards while identifying normative gaps and regulatory inconsistencies affecting the effectiveness of criminal asset recovery.

Secondary legal materials consist of peer-reviewed journal articles indexed in Scopus and Web of Science, scholarly books, research reports, doctoral dissertations, policy papers, and official publications issued by the FATF, OECD, International Monetary Fund (IMF), World Bank, United Nations Office on Drugs and Crime (UNODC), Europol, the Basel Institute on Governance, and other international organisations. These sources provide the theoretical foundation for the study, support the comparative analysis, and facilitate a critical examination of international developments in digital asset recovery. Tertiary legal materials, including legal dictionaries, legal encyclopaedias, legislative indexes, and other authoritative reference sources, are used to ensure terminological consistency, clarify legal concepts, and enhance the accuracy of the interpretation of technical legal terminology employed throughout the research.

Legal Material Collection Techniques and Legal Material Analysis Techniques

The collection of legal materials in this study was conducted through library research, systematically organised to address legal issues concerning the recovery of criminal assets in digital financial crime. Consistent with the doctrinal legal research methodology, the study relies on the identification, retrieval, selection, and critical examination of relevant legal sources rather than field observations or interviews. This approach reflects the doctrinal understanding of law as a normative system whose coherence, structure, substance, and underlying principles are analysed in response to contemporary legal challenges (Van Hoecke, 2011; Hutchinson & Duncan, 2012).

The initial stage involved compiling and reviewing Indonesia's statutory framework governing criminal offences, money laundering, electronic transactions, personal data protection, financial sector regulation, digital assets, and the powers of law enforcement agencies and financial supervisory authorities. The analysis was subsequently extended to international legal instruments, including the Financial Action Task Force (FATF) Recommendations, the FATF Guidance on Virtual Assets and Virtual Asset Service Providers, the United Nations Convention against Corruption (UNCAC), the United Nations Convention against Transnational Organized Crime (Palermo Convention), together with other international standards governing asset recovery, beneficial ownership, virtual assets, and cross-border cooperation. These materials were examined to assess the degree of harmonisation between Indonesia's legal framework and international standards while identifying areas requiring legal reform in response to the evolution of digital financial crime.

In addition to primary legal materials, the study draws upon secondary sources comprising peer-reviewed journal articles indexed in Scopus and Web of Science, academic books, doctoral dissertations, research reports, and policy publications issued by the Financial Action Task Force (FATF), the Organisation for Economic Co-operation and Development (OECD), the International Monetary Fund (IMF), the World Bank, the United Nations Office on Drugs and Crime (UNODC), Europol, the Basel Institute on Governance, and other international organisations. The literature review was conducted using major academic databases, including Scopus, Web of Science, HeinOnline, SpringerLink, ScienceDirect, Taylor & Francis Online, Wiley Online Library, and Google Scholar as a supplementary source. These resources provided the theoretical foundation for the study, identified international best practices, and captured recent regulatory developments concerning digital asset recovery.

To ensure academic rigour and reliability, the literature selection process was guided by four principal criteria. First, relevance, requiring that each source directly address issues relating to criminal liability, asset recovery, digital assets, blockchain technology, money laundering, beneficial ownership, or the FATF standards. Secondly, authoritativeness, prioritising publications from internationally recognised academic journals, reputable international organisations, and applicable legislation. Thirdly, currency, with preference given to publications produced between 2021 and 2026 to ensure that the analysis reflects recent developments in digital asset regulation, blockchain-based investigations, and AML/CFT reform. Finally, analytical contribution was considered by assessing the extent to which each source strengthened the study's theoretical framework, normative reasoning, and comparative analysis. These selection criteria were intended to ensure that the legal materials used in the research were relevant, credible, and academically robust.

The legal materials were analysed using a qualitative doctrinal approach, which conceptualises law as an integrated system of legal norms, principles, doctrines, and values. Rather than examining causal relationships through statistical methods, the analysis evaluates whether the existing legal framework satisfies the principles of coherence, consistency, legal certainty, and effectiveness in facilitating the recovery of criminal assets derived from digital financial crime. Consequently, the analysis extends beyond describing statutory provisions to assessing their adequacy, identifying regulatory deficiencies, and developing prescriptive legal arguments for reform.

The first stage of the analysis involved the identification and classification of legal norms relating to criminal liability, asset tracing, freezing, seizure, confiscation, asset management, and the recovery of criminal proceeds. This process sought to identify the relationships among legal instruments, determine the scope of existing regulation, and detect regulatory overlaps or normative gaps that affect the effectiveness of asset recovery. Each legal instrument was examined as part of Indonesia's broader criminal justice framework in order to assess its overall coherence and institutional integration.

The study subsequently applied several recognised methods of legal interpretation commonly employed in doctrinal legal research. Grammatical interpretation was used to determine the ordinary meaning of legal provisions concerning digital assets, seizure, and confiscation. Systematic interpretation examined the interrelationship among statutory provisions to identify regulatory consistency and normative conflicts. Historical interpretation explored the legislative background and purpose underlying the enactment of relevant legal provisions, while teleological interpretation assessed whether their objectives remain compatible with technological innovation and contemporary digital financial crime. In addition, comparative interpretation was employed to evaluate Indonesia's legal framework against jurisdictions that have developed more advanced digital asset recovery mechanisms, thereby identifying legal principles and best practices suitable for adaptation within Indonesia's civil law system.

The analysis further incorporated vertical and horizontal harmonisation. Vertical harmonisation examined the consistency of domestic legislation with Indonesia's constitutional principles and its international legal obligations. Horizontal harmonisation evaluated the coherence among criminal law, criminal procedure, financial regulation, cyber law, and digital asset legislation. Such analysis is essential because digital financial crime is inherently multidimensional and requires an integrated legal framework capable of responding to its complex characteristics.

The final stage consisted of a normative evaluation of Indonesia's legal framework against international standards, particularly the FATF Recommendations concerning asset recovery, confiscation, beneficial ownership, virtual assets, and international cooperation. This evaluation compared Indonesia's legal provisions with internationally recognised principles, identified regulatory gaps, and synthesised the findings to formulate recommendations for legal reform. Accordingly, the analysis is both evaluative and prescriptive, seeking not only to identify deficiencies within the existing legal framework but also to propose a reconstructed asset recovery regime that is more effective, technologically adaptive, and aligned with international standards and the principles of the Rule of Law.

Analytical Framework and Legal Reconstruction Model

This study employs an integrated analytical framework that combines legal theory, normative analysis, and international standards to evaluate the effectiveness of Indonesia's criminal asset recovery regime in addressing digital financial crime. The framework is founded on the premise that asset recovery cannot be adequately understood from a single disciplinary perspective, as it involves the interaction of substantive criminal law, criminal procedure, financial regulation, blockchain technology, digital asset governance, and international cooperation. Accordingly, the study integrates complementary theoretical perspectives to produce a comprehensive normative evaluation while providing the foundation for a legal reform model capable of responding to technological innovation and the evolving nature of digital financial crime.

The primary analytical foundation is Criminal Liability Theory, which is used to examine the relationship between criminal responsibility and asset recovery mechanisms. Within this study, criminal liability is understood not only as the legal basis for imposing criminal sanctions but also as the legal justification for tracing, freezing, seizing, confiscating, and recovering the proceeds of crime. This perspective facilitates an assessment of whether Indonesia's legal framework adequately connects the establishment of criminal liability with the State's authority to recover assets derived from unlawful conduct, including digital assets stored or transferred through blockchain networks.

This analysis is further informed by Asset Recovery Theory, which regards asset recovery as a central objective of the modern criminal justice system. Under this theoretical framework, the effectiveness of law enforcement is measured not only by the successful prosecution of offenders but also by the State's capacity to deprive them of the economic benefits generated through criminal activity. Accordingly, the study evaluates whether Indonesia's legal framework provides effective mechanisms for identifying, tracing, freezing, seizing, managing, and recovering criminal assets, including virtual assets characterised by decentralisation, pseudonymity, and cross-border mobility.

The study also applies Economic Analysis of Law to assess the efficiency of the regulatory framework in reducing the economic incentives for crime. This approach is based on the assumption that perpetrators of digital financial crime act rationally by weighing potential benefits against associated risks. Consequently, the effectiveness of the legal system depends not only on the severity of criminal sanctions but also on its ability to increase the economic costs of offending through timely, enforceable, and effective asset seizure and confiscation mechanisms. Within this context, the research examines the extent to which Indonesia's legal framework is capable of producing an effective economic deterrent through a robust asset recovery regime.

To ensure that asset recovery remains consistent with the principles of a constitutional state governed by law, the analysis further incorporates Rule of Law Theory and Corrective Justice Theory. Rule of Law Theory provides the normative basis for evaluating whether state powers to trace, freeze, and seize digital assets comply with the principles of legality, legal certainty, proportionality, accountability, and effective judicial oversight. Corrective Justice

Theory, in turn, is employed to assess the extent to which asset recovery mechanisms facilitate the restoration of losses suffered by the State and victims, thereby re-establishing legal equilibrium. From this perspective, asset recovery is understood not merely as a punitive measure but as an essential instrument for achieving substantive justice and strengthening public confidence in the criminal justice system.

Given the rapid pace of technological development, the study also integrates Progressive Law Theory and Law and Technology Theory to evaluate the capacity of legal institutions to respond to technological innovation. Particular attention is devoted to the use of blockchain technology, blockchain analytics, and digital investigative technologies as law enforcement tools, while ensuring full compliance with the principles of Due Process of Law, the protection of human rights, and the right to privacy.

As an international benchmark, the study adopts the Financial Action Task Force (FATF) Recommendations to evaluate Indonesia's legal framework with respect to asset recovery, confiscation, beneficial ownership transparency, the regulation of Virtual Asset Service Providers (VASPs), the risk-based approach, and international cooperation. The FATF standards serve as an objective normative benchmark for assessing the extent to which Indonesia's legal framework is harmonised with the global anti-money laundering and counter-terrorist financing (AML/CFT) regime.

Building upon this analytical framework, the study develops the Integrated Digital Asset Recovery Framework (IDARF) as a model for reconstructing Indonesia's criminal asset recovery regime. IDARF integrates legal doctrine, statutory analysis, comparative legal practice, technological developments, and the FATF standards into a unified framework that positions asset recovery as a strategic objective throughout every stage of the criminal justice process—from investigation and prosecution to the execution of judicial decisions.

Conceptually, IDARF consists of six interconnected components: (1) strengthening Criminal Liability as the legal basis for asset tracing and confiscation; (2) implementing Digital Asset Tracing through blockchain analytics; (3) establishing effective Beneficial Ownership Verification mechanisms; (4) harmonising Indonesia's legal framework with the FATF Recommendations; (5) strengthening International Cooperation through Mutual Legal Assistance (MLA), financial intelligence exchange, and joint investigations; and (6) ensuring the consistent application of Due Process of Law and the protection of human rights throughout every stage of the asset recovery process.

Accordingly, the Integrated Digital Asset Recovery Framework (IDARF) represents the principal conceptual contribution of this study. By integrating criminal law, digital technology, and international regulatory standards within a coherent legal framework, the model seeks to enhance the effectiveness of criminal asset recovery, strengthen legal certainty, and support the ongoing reform of Indonesia's criminal justice system in responding to the evolving challenges posed by digital financial crime.

Digital Financial Crime

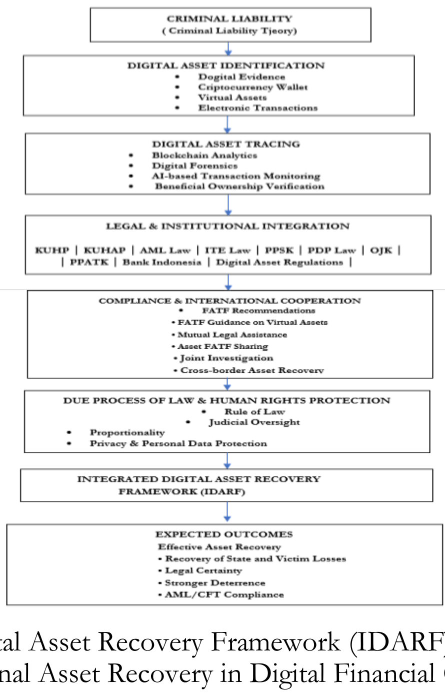

Figure 1. Integrated Digital Asset Recovery Framework (IDARF): An Integrated Model for Criminal Asset Recovery in Digital Financial Crime.

The Integrated Digital Asset Recovery Framework (IDARF) conceptualises asset recovery in digital financial crime as an integrated legal process extending from the initial investigation through to the enforcement of judicial decisions. The process begins with the establishment of the underlying criminal offence and Criminal Liability, which provide the legal basis for asset tracing, freezing, seizure, and confiscation. The subsequent stage involves the identification of digital assets through electronic evidence, virtual assets, cryptocurrency wallets, and digital transactions, supported by Digital Asset Tracing, Blockchain Analytics, Digital Forensics, and Beneficial Ownership Verification. These mechanisms are further reinforced through the harmonisation of Indonesia's legal framework with the Financial Action Task Force (FATF) Recommendations and strengthened international cooperation, including Mutual Legal Assistance (MLA), Joint Investigations, and cross-border asset recovery. Throughout every stage, the framework operates in accordance with the principles of the Rule of Law, Due Process of Law, and the protection of human rights, thereby establishing an asset recovery regime that is effective, technologically adaptive, and aligned with internationally recognised legal standards.

4. Results and Discussion

Regulatory Weaknesses in Indonesia's Criminal Asset Recovery Framework: A Normative Analysis of the Criminal Code, Criminal Procedure Code, AML Law, ITE Law, PPSK Law, and Personal Data Protection Law

The effectiveness of asset recovery in digital financial crime depends on the integration of Criminal Liability, investigative powers, asset tracing mechanisms, and the confiscation of criminal proceeds. In Indonesia, however, these elements remain regulated through fragmented and sector-specific legislation that has evolved incrementally and is ill-equipped to address the distinctive characteristics of digital assets, including their cross-border mobility, pseudonymity, and reliance on distributed ledger technology (DLT). Consequently, law enforcement continues to emphasise an offender-oriented approach, focusing primarily on establishing criminal liability, while an asset-oriented approach has yet to receive adequate normative support. This imbalance undermines the effectiveness of combating digital financial crime, as offenders may continue to retain illicit economic gains despite being convicted and sentenced.

From the perspective of Criminal Liability Theory, criminal responsibility should extend beyond providing the legal basis for punishment to legitimising the State's authority to trace, freeze, seize, and confiscate criminal assets. Indonesia's legal framework, however, continues to treat criminal liability and asset recovery as largely separate legal regimes. Although Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering significantly broadened the legal basis for asset confiscation, its implementation remains dependent upon the Indonesian Code of Criminal Procedure (KUHAP), which was originally designed to regulate tangible property. As a result, digital assets transferred through cryptocurrency wallets, smart contracts, or decentralised finance (DeFi) protocols remain inadequately regulated with respect to seizure and preservation, creating a substantial gap between the sophistication of contemporary financial crime and the procedural capacity of Indonesia's criminal justice system.

This disconnect is further reflected in the relationship between the Indonesian Criminal Code (Law No. 1 of 2023) and the Code of Criminal Procedure (KUHAP). While the new Criminal Code introduces significant reforms to Indonesia's substantive criminal law, these developments have not been accompanied by corresponding procedural reforms governing the identification, freezing, seizure, management, and confiscation of digital assets. The resulting inconsistency between substantive and procedural criminal law limits the ability of law enforcement authorities to secure blockchain-based assets effectively. Consequently, digital assets remain vulnerable to transfer beyond Indonesia's jurisdiction during the course of criminal investigations and judicial proceedings.

A similar degree of fragmentation exists between the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, and Law No. 27 of 2022 concerning Personal Data Protection. Although these statutes pursue distinct regulatory objectives, they increasingly intersect in the enforcement of digital financial crime. The absence of an integrated legal framework has created uncertainty regarding the authority of law enforcement agencies to access and utilise electronic data for asset tracing purposes. On the one hand, effective investigations require timely access to transaction records and digital identity information. On the other, personal data protection legislation requires strict compliance with the principles of legality, proportionality, and accountability. This regulatory tension illustrates that Indonesia's sector-specific legislation has yet to achieve an appropriate balance between effective law enforcement and the protection of constitutional rights.

From the standpoint of Rule of Law Theory, this fragmentation weakens both legal certainty and regulatory consistency. The Rule of Law requires that any restriction upon property rights or the right to privacy be based upon clear legal authority, established procedures, and effective judicial oversight. Yet the dispersal of powers relating to asset tracing, freezing, and seizure across multiple legislative instruments has produced inconsistent interpretations regarding the scope of law enforcement authority. At the same time, individuals subjected to investigative measures face considerable uncertainty regarding the legal safeguards and remedies available to challenge asset seizure. Accordingly, the principal challenge lies not merely in the inadequacy of individual legal provisions but in the absence of a coherent regulatory framework capable of ensuring both the effectiveness and legitimacy of digital asset recovery.

These structural weaknesses are equally evident when examined through the lens of Asset Recovery Theory, which regards asset recovery as the primary mechanism for depriving offenders of the economic benefits derived from criminal conduct. From this perspective, the success of the criminal justice system should be measured not only by the prosecution of offenders but also by the State's capacity to identify, trace, freeze, seize, and confiscate criminal proceeds. Indonesia's legal framework, however, continues to prioritise offender prosecution, while mechanisms for identifying and securing criminal assets remain insufficiently integrated during the early stages of criminal investigations. Consequently, digital assets are frequently transferred through multiple cryptocurrency wallets, mixing services, or foreign jurisdictions before freezing measures can be implemented. These circumstances demonstrate that the limitations of Indonesia's asset recovery regime stem not only from procedural deficiencies but also from a regulatory design that has failed to keep pace with the speed of digital transactions and the transnational nature of contemporary financial crime.

From a normative perspective, the interaction between the Indonesian Criminal Code, the Code of Criminal Procedure, the Money Laundering Law, the Electronic Information and Transactions Law, the Financial Sector Development and Strengthening Law, and the Personal Data Protection Law continues to reflect significant regulatory fragmentation. Although each statute governs a specific aspect of digital financial regulation, none establishes a comprehensive framework integrating Criminal Liability, digital investigation, personal data protection, financial sector governance, and asset confiscation within a unified legal system. Consequently, the effectiveness of law enforcement depends largely upon inter-agency coordination and administrative interpretation rather than upon a coherent legislative framework. These shortcomings underscore the need for comprehensive legal reconstruction capable of integrating criminal law, digital asset tracing technologies, and international asset recovery standards in order to establish a more effective, adaptive, and legally certain asset recovery regime.

Challenges in Digital Asset Tracing, Beneficial Ownership, and Institutional Coordination

The rapid expansion of cryptocurrency, virtual assets, and decentralised finance (DeFi) has fundamentally transformed the paradigm of criminal asset recovery from conventional tangible assets to blockchain-based digital assets. Unlike traditional assets that can generally be traced through the banking system, digital assets are characterised by decentralisation, pseudonymity, and cross-border mobility, making asset tracing significantly more challenging. Indonesia's existing legal framework, which remains largely designed for conventional financial systems, has yet to accommodate these distinctive characteristics. Consequently, criminal proceeds transferred through cryptocurrencies, mixing services, cross-chain bridges, or non-custodial wallets have become increasingly difficult to identify and recover.

These challenges are compounded by weaknesses in the current beneficial ownership regime. Although transparency requirements have been introduced, their implementation remains primarily focused on legal entities and regulated financial institutions. In practice, offenders frequently exploit shell companies, nominee arrangements, fraudulent digital identities, and anonymous cryptocurrency wallets to conceal the true ownership and control of illicit assets. As a result, legal ownership often fails to reflect actual economic control, thereby undermining the primary objective of asset recovery—namely, depriving offenders of the economic benefits derived from criminal activity.

The integration of blockchain investigation into Indonesia's criminal justice system also remains underdeveloped. While blockchain transactions are inherently transparent, effective tracing requires sophisticated blockchain analytics, digital forensics, and specialised expertise capable of linking digital wallet addresses to identifiable individuals. International studies consistently demonstrate that asset recovery becomes substantially more effective when legal authority is complemented by advanced analytical technologies and close cooperation with Virtual Asset Service Providers (VASPs). By contrast, conventional investigative methods struggle to keep pace with blockchain transactions conducted in real time across multiple jurisdictions.

From the perspective of Law and Technology, the effectiveness of legal regulation depends upon its capacity to incorporate technological innovation into criminal investigations and evidentiary processes. Legal reform, therefore, cannot be achieved solely through legislative amendment but must also include institutional capacity-building and the adoption of digital investigative technologies. This approach is consistent with Economic Analysis of Law, which suggests that strengthening the State's ability to trace and confiscate criminal assets significantly increases the economic risks associated with offending, thereby enhancing the deterrent effect of criminal law.

Another significant weakness concerns the legal framework governing digital asset confiscation. Indonesia's criminal procedure legislation does not yet provide comprehensive rules governing the freezing, custody, management, and enforcement of digital assets. Unlike physical property, digital assets require secure management of private keys, the use of secure custodial wallets, and procedural safeguards to preserve both the integrity and market value of assets throughout criminal proceedings. The absence of such regulations increases the risk of asset loss and value depreciation resulting from market volatility.

Institutional coordination also remains fragmented. Although the Financial Transaction Reports and Analysis Centre (PPATK), the Indonesian National Police, the Office of the Attorney General, the Financial Services Authority (OJK), and Bank Indonesia exercise complementary responsibilities, information sharing remains largely sectoral and is not supported by integrated real-time data exchange mechanisms. Consequently, asset tracing efforts frequently lag behind the rapid movement of digital assets across blockchain networks, significantly reducing the effectiveness of asset recovery.

Comparative experience from other jurisdictions demonstrates the advantages of a more integrated approach. The United Kingdom has expanded its powers to seize cryptocurrency assets under the Proceeds of Crime Act; Singapore has incorporated the supervision of digital asset service providers within the Payment Services Act; the United States has strengthened enforcement through collaboration with blockchain analytics providers; and the European Union has enhanced beneficial ownership transparency and cross-border cooperation. Although these jurisdictions employ different regulatory models, each recognises the integration of legal regulation, investigative technology, and institutional coordination as the foundation of an effective digital asset recovery regime.

A synthesis of the international literature published between 2021 and 2026 confirms that effective asset recovery in the digital era depends upon the integration of blockchain analytics, beneficial ownership verification, cross-border cooperation, and financial intelligence sharing. Nevertheless, existing scholarship generally examines these components in isolation, resulting in the absence of a comprehensive and integrated legal framework. Addressing this gap, the present study proposes the Integrated Digital Asset Recovery Framework (IDARF), which combines Criminal Liability, Digital Asset Tracing, blockchain technology, compliance with the Financial Action Task Force (FATF) Recommendations, and inter-agency coordination into a unified normative framework designed to strengthen the effectiveness of asset recovery in combating digital financial crime in Indonesia.

Comparative Analysis of Criminal Asset Recovery: Lessons from the United Kingdom, Singapore, and Australia

A synthesis of the international literature published between 2021 and 2026 demonstrates that the effectiveness of asset recovery in the digital era depends upon the integration of blockchain analytics, beneficial ownership verification, cross-border cooperation, and financial intelligence sharing. Nevertheless, most existing studies examine these elements in isolation, resulting in the absence of a comprehensive legal framework. To address this gap, the present study proposes the Integrated Digital Asset Recovery

Framework (IDARF) as a normative model that integrates Criminal Liability, Digital Asset Tracing, blockchain technology, compliance with the Financial Action Task Force (FATF) Recommendations, and inter-agency coordination to strengthen the effectiveness of asset recovery in combating digital financial crime in Indonesia.

A comparative analysis of the United Kingdom, Singapore, and Australia reveals differences in institutional design while identifying four common characteristics. First, asset recovery is recognised as an integral component of crime control policy rather than merely a consequence of criminal conviction. Secondly, blockchain analytics has been institutionalised as a core investigative tool supporting both evidentiary processes and the tracing of digital assets. Thirdly, beneficial ownership transparency has become a critical mechanism for uncovering concealed assets held through shell companies, nominee arrangements, or complex ownership structures. Finally, effective coordination among law enforcement agencies, financial authorities, and digital asset regulators is achieved through integrated information-sharing mechanisms, enabling the identification, freezing, and seizure of criminal assets at a pace that can keep up with transfers occurring across blockchain networks.

These findings are consistent with broader developments in international scholarship between 2021 and 2026, which demonstrate a shift from purely doctrinal legal approaches towards integrated frameworks combining law, technology, and digital financial governance. Numerous studies emphasise that the successful confiscation of cryptocurrency assets depends upon institutional capacity in digital forensics, transparency of beneficial ownership, and effective cross-border cooperation. Research on cryptocurrency confiscation further indicates that expanding confiscation powers alone is insufficient without clear procedures governing the management of digital assets, including the secure custody of private keys, asset valuation, and mechanisms for mitigating cryptocurrency price volatility. Likewise, studies of blockchain investigations demonstrate that the transparency of blockchain networks can become a significant advantage for law enforcement when supported by analytical tools capable of linking transaction patterns to identifiable offenders and organised criminal networks.

Despite these developments, existing scholarship continues to examine asset recovery, cryptocurrency confiscation, and blockchain investigations as distinct fields of inquiry. Research integrating these three dimensions within a comprehensive framework for legal reform remains limited, particularly in jurisdictions operating under civil law traditions such as Indonesia. Consequently, the experiences of the United Kingdom, Singapore, and Australia are not presented as models for direct legal transplantation but rather as normative reference points for strengthening regulatory harmonisation, enhancing technological investigative capacity, and improving institutional coordination. Building upon these comparative insights, this study develops the Integrated Digital Asset Recovery Framework (IDARF) as a comprehensive legal framework that integrates Criminal Liability, Digital Asset Tracing, blockchain technology, and the FATF Recommendations, while remaining firmly grounded in the principles of the Rule of Law, Due Process of Law, and the protection of human rights.

Comparative Perspectives from the United States, Switzerland, and the European Union

Beyond the experiences of the United Kingdom, Singapore, and Australia, developments in digital asset recovery regimes in the United States, Switzerland, and the European Union further demonstrate that effective responses to digital financial crime depend upon the integration of legal frameworks, technological innovation, and institutional governance. Although each jurisdiction has adopted regulatory approaches reflecting its own legal tradition, they share a common objective: preventing offenders from retaining the proceeds of crime through the use of cryptocurrencies, virtual assets, and other digital financial instruments.

The United States has adopted a highly progressive approach through a combination of criminal forfeiture, civil forfeiture, and non-conviction-based confiscation. The Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Internal Revenue Service–Criminal Investigation (IRS-CI), and the Financial Crimes Enforcement Network (FinCEN) have established an integrated investigative framework that incorporates blockchain analytics, digital forensics, and financial intelligence. The successful recovery of assets in major cases—including Silk Road, the Bitfinex Hack, and numerous ransomware investigations—demonstrates that effective asset recovery no longer depends on physical possession of evidence, but rather on the ability to identify private keys, trace blockchain transactions, and establish the connection between cryptocurrency wallet addresses and criminal offenders.

These experiences illustrate that blockchain technology represents not only a challenge for law enforcement but also a valuable evidentiary resource when supported by advanced analytical capabilities.

Switzerland has adopted a different model centred on legal certainty, financial market stability, and compliance with international anti-money laundering standards. Under the supervision of the Swiss Financial Market Supervisory Authority (FINMA), digital assets are regulated through a comprehensive risk-based approach. Mandatory beneficial ownership verification, together with regulatory oversight of Virtual Asset Service Providers (VASPs), enhances the ability of authorities to identify suspicious transactions before assets are transferred to foreign jurisdictions. Unlike more enforcement-oriented models, Switzerland places greater emphasis on regulatory compliance, market transparency, and preventive supervision as integral elements of its asset recovery strategy. Consequently, asset recovery begins not after the commission of an offence but at the preventive stage through a robust compliance framework.

The European Union has pursued regulatory harmonisation through a range of supranational legal instruments, including the Anti-Money Laundering (AML) Package, the establishment of the Anti-Money Laundering Authority (AMLA), and the implementation of the Markets in Crypto-Assets Regulation (MiCA). These initiatives aim to establish uniform standards governing virtual asset supervision, beneficial ownership transparency, and inter-agency information exchange. Given the inherently transnational nature of digital financial crime, effective asset recovery depends upon the interoperability of legal systems and the capacity to freeze and seize assets rapidly across multiple jurisdictions. This approach reflects a broader transition from voluntary cooperation towards a more institutionalised model of regional governance.

The comparative analysis demonstrates that Indonesia's principal challenge lies not in the absence of legislation governing money laundering or asset confiscation, but in the lack of an integrated legal architecture that connects Criminal Liability, digital investigative technologies, financial sector supervision, and international cooperation. Indonesia's current regulatory framework remains characterised by fragmented institutional authority and sector-specific regulation, whereas the comparator jurisdictions have developed integrated models combining financial intelligence, blockchain analytics, beneficial ownership verification, and asset confiscation within a unified enforcement framework. These findings suggest that meaningful legal reform in Indonesia requires comprehensive institutional reconstruction and regulatory harmonisation rather than isolated amendments to individual statutes.

Figures and Tables

Table 1. Comparative Legal Analysis of Digital Asset Recovery Frameworks.

Analytical Aspect	Indonesia	United States	Switzerland	European Union
Asset Recovery Legal Framework	Fragmented across the Code of Criminal Procedure (KUHAP), the Anti-Money Laundering Law, the Electronic Information and Transactions Law, and the Financial Sector Development and Strengthening Law	Integrated through criminal forfeiture, civil forfeiture, and non-conviction-based confiscation	Integrated within the financial regulatory framework	Harmonised through the Anti-Money Laundering (AML) Package and the Markets in Crypto-Assets Regulation (MiCA)
Blockchain Investigation	No explicit legal framework governing blockchain-based investigations	Widely utilised in federal criminal investigations	Supported by financial regulators and financial institutions	Increasingly implemented through coordinated action among competent authorities
Beneficial Ownership	Implementation remains limited and fragmented	Embedded as a core component of financial investigations	Subject to stringent beneficial ownership verification requirements	Strengthened through transparent beneficial

				ownership registers
Regulation of Virtual Asset Service Providers (VASPs)	Regulatory framework remains under development	Supervised under the Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) regime	Regulated by the Swiss Financial Market Supervisory Authority (FINMA)	Comprehensively regulated under MiCA
Digital Asset Confiscation	No dedicated legal procedures governing the seizure and confiscation of digital assets	Well-established procedures for the seizure, management, and confiscation of digital assets	Supported by comprehensive financial compliance regulations	Integrated with cross-border asset recovery and judicial cooperation mechanisms
Institutional Coordination	Predominantly sector-based with fragmented institutional responsibilities	Multi-agency task force model involving federal law enforcement agencies	Strong institutional coordination between financial regulators and law enforcement authorities	Institutionalised regional cooperation among Member States and EU agencies
International Cooperation	Primarily reliant on conventional Mutual Legal Assistance (MLA) mechanisms	Extensive participation in joint investigations and international enforcement cooperation	Conducted in accordance with FATF standards and international cooperation frameworks	

A synthesis of the international literature published between 2021 and 2026 indicates that the effectiveness of digital asset recovery is founded upon four interrelated pillars: regulatory integration, the application of blockchain analytics, beneficial ownership transparency, and strengthened cross-border cooperation. Although there is broad scholarly consensus regarding the importance of these elements, existing research has largely examined them in isolation or within the context of individual jurisdictions. Consequently, a significant conceptual gap remains in the development of a normative framework that integrates Criminal Liability, digital asset tracing technologies, institutional governance, and compliance with the **Financial Action Task Force (FATF)

5. Conclusion

This study demonstrates that the limited effectiveness of criminal asset recovery in addressing digital financial crime in Indonesia is attributable not merely to deficiencies in substantive legal norms, but more fundamentally to institutional fragmentation and the absence of an integrated framework linking Criminal Liability, digital asset tracing, technology-driven investigations, and international cooperation. Although the legal basis for asset recovery is dispersed across the Indonesian Criminal Code, the Code of Criminal Procedure, Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, and the Personal Data Protection Law, these instruments have yet to establish a coherent legal regime capable of addressing the distinctive characteristics of cryptocurrencies, virtual assets, and blockchain-based transactions. Consequently, the State's capacity to trace, freeze, seize, and recover criminal assets has not kept pace with the rapid evolution of digital financial technologies.

The evaluation against the Financial Action Task Force (FATF) Recommendations further indicates that Indonesia has incorporated the core principles of the anti-money laundering and counter-terrorist financing (AML/CFT) regime, including the risk-based approach, strengthened financial intelligence, and enhanced beneficial ownership transparency. Nevertheless, significant implementation challenges remain in the regulation of virtual assets, blockchain-based investigations, digital asset confiscation, and the effectiveness of cross-border cooperation. These findings suggest that Indonesia's principal challenge no longer lies in its formal commitment to international standards, but rather in the institutional capacity and regulatory harmonisation required to translate those standards into effective law enforcement practice.

Building upon these findings, this study proposes the Integrated Digital Asset Recovery Framework (IDARF) as a comprehensive model for legal reconstruction. The framework integrates Criminal Liability, Digital Asset Tracing, Blockchain Analytics, Beneficial Ownership Verification, compliance with the FATF Recommendations, international cooperation, the principles of Due Process of Law, the protection of human rights, and a clear commitment to recovering losses suffered by both the State and victims. Unlike conventional approaches that treat asset recovery as a post-conviction consequence, IDARF positions asset recovery as an integral objective throughout every stage of the criminal justice process. By integrating legal, technological, and institutional dimensions within a single normative framework, the model offers a more adaptive response to the evolving nature of digital financial crime while strengthening the effectiveness of Indonesia's criminal justice system in the digital economy.

This study makes several conceptual contributions to the development of criminal law and digital economic law. First, from the perspective of Criminal Liability Theory, it extends the traditional understanding of criminal liability by positioning digital asset recovery as an integral objective of criminal justice. Within this framework, criminal liability serves not only as the legal basis for imposing sanctions on offenders but also as the normative justification for depriving them of the economic benefits derived from criminal conduct.

Secondly, the study advances Asset Recovery Theory by expanding the conventional concept of asset recovery into a broader framework of digital asset recovery capable of addressing the distinctive characteristics of cryptocurrencies, blockchain technology, and virtual assets. From this perspective, effective asset recovery depends not merely on the legal authority to seize and confiscate assets, but also on the capacity of the legal system to integrate digital asset tracing technologies, beneficial ownership verification, and effective mechanisms for cross-border cooperation.

Thirdly, the study contributes to the growing field of Law and Technology by demonstrating that blockchain analytics, digital forensics, and artificial intelligence should be recognised not merely as technical investigative tools but as normative components of modern criminal procedure. This approach is consistent with the principles of Progressive Law, which require legal systems to adapt to social and technological change while remaining firmly grounded in the Rule of Law, Due Process of Law, and the protection of human rights. From the perspective of Economic Analysis of Law, the proposed Integrated Digital Asset Recovery Framework (IDARF) also enhances the efficiency of law enforcement by strengthening the State's capacity to trace and confiscate criminal assets, thereby increasing the deterrent effect of criminal law while improving the recovery of losses suffered by both the State and victims. Accordingly, the principal contribution of this study extends beyond proposing regulatory reform; it offers a coherent conceptual framework that integrates criminal law theory, digital technology, and international financial governance standards into a unified model for digital asset recovery.

The findings of this study carry significant practical implications for the reform of Indonesia's criminal justice system and the governance of the digital financial sector. For policymakers and legislators, the study demonstrates that meaningful legal reform cannot be achieved through isolated amendments to individual statutes. Instead, it requires the harmonisation of substantive criminal law, criminal procedure, the anti-money laundering (AML/CFT) regime, financial sector regulation, and personal data protection within a coherent legal framework capable of addressing the multifaceted nature of digital financial crime.

For law enforcement agencies—particularly the Indonesian National Police, the Office of the Attorney General, and the Financial Transaction Reports and Analysis Centre (PPATK)—the findings underscore the need to transition from conventional investigative methods to technology-driven enforcement strategies. The systematic use of blockchain analytics, digital forensics, artificial intelligence-based transaction analysis, and integrated financial intelligence should become standard components of criminal investigations involving digital assets. At the judicial level, the Supreme Court of Indonesia should consider developing judicial guidelines governing electronic evidence, the seizure and confiscation of digital assets, and the protection of third-party rights in order to promote greater consistency in judicial decision-making.

The study also has important implications for the Financial Services Authority (OJK), Bank Indonesia, cryptocurrency exchanges, and Virtual Asset Service Providers (VASPs). Regulatory measures such as Know Your Customer (KYC) requirements, Customer Due

Diligence (CDD) procedures, suspicious transaction reporting, and beneficial ownership verification should be regarded as fundamental mechanisms for preventing digital financial crime rather than merely as regulatory compliance obligations. From an academic perspective, the study provides a comprehensive conceptual framework for future research at the intersection of criminal law, digital technology, and global financial governance, while reinforcing the understanding that effective asset recovery constitutes an essential mechanism for protecting both public interests and the rights of victims of crime.

Based on the findings of this study, Indonesia's criminal law reform should be directed towards establishing an integrated, adaptive, and technology-responsive asset recovery regime. The foremost legislative priority is the revision of the Indonesian Code of Criminal Procedure (KUHAP) to incorporate comprehensive procedures governing the freezing, seizure, management, and enforcement of digital assets. Such reform should be harmonised with Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the Electronic Information and Transactions Law, Law No. 4 of 2023 concerning Financial Sector Development and Strengthening, and the Personal Data Protection Law. The revised framework should also provide clear legal standards for the admissibility of digital evidence, the use of blockchain analytics in criminal investigations, and the protection of human rights through the consistent application of Due Process of Law and effective judicial oversight.

Beyond revising existing legislation, this study recommends the enactment of a dedicated Digital Asset Recovery Act to establish a comprehensive legal framework governing the identification, tracing, freezing, seizure, management, and recovery of digital assets. The proposed legislation should incorporate provisions on beneficial ownership transparency, the regulation of Virtual Asset Service Providers (VASPs), non-conviction-based confiscation consistent with constitutional safeguards, and procedures governing cross-border cooperation in asset recovery proceedings.

From an institutional perspective, the Government should consider establishing a Digital Asset Recovery Center as a national coordination body bringing together the Financial Transaction Reports and Analysis Centre (PPATK), the Indonesian National Police, the Office of the Attorney General, the Financial Services Authority (OJK), Bank Indonesia, the Ministry of Finance, and the Ministry of Communication and Digital Affairs. This institution would function as the central hub for financial intelligence sharing, the development of digital investigative technologies, and the coordination of cross-sector asset recovery operations. Its effectiveness should be supported by advanced technological infrastructure, including blockchain analytics, digital forensic laboratories, an integrated beneficial ownership registry, and a comprehensive integrated financial intelligence system.

At the international level, Indonesia should strengthen the implementation of Mutual Legal Assistance (MLA), expand its participation in Joint Investigation Teams (JITs), and deepen cooperation through the Egmont Group, INTERPOL, and regional ASEAN mechanisms to accelerate the tracing and recovery of assets across jurisdictions. Collectively, these recommendations support the implementation of the Integrated Digital Asset Recovery Framework (IDARF) as a comprehensive model of legal reform that integrates Criminal Liability, technological innovation, compliance with the Financial Action Task Force (FATF) Recommendations, and the protection of human rights. Through this integrated approach, Indonesia's asset recovery regime will be better equipped to respond to the evolving challenges of digital financial crime while strengthening the integrity of the criminal justice system and the stability of the national financial sector.

As with doctrinal legal research generally, this study has several limitations that should be considered when interpreting its findings and contributions. First, the research adopts a doctrinal legal research approach centred on the analysis of legal norms, doctrinal scholarship, academic literature, and national and international legal instruments. Consequently, it does not empirically assess the effectiveness of digital asset recovery mechanisms as implemented by law enforcement agencies or financial regulatory authorities. The findings therefore focus primarily on evaluating the adequacy, coherence, and consistency of the existing legal framework rather than measuring institutional performance in practice.

Secondly, the study does not incorporate empirical methods such as in-depth interviews, focus group discussions, or case studies involving investigators, prosecutors, judges, the Financial Transaction Reports and Analysis Centre (PPATK), financial regulators, or Virtual Asset Service Providers (VASPs). The perspectives of these stakeholders could provide valuable insights into the operational challenges associated with tracing, seizing, and recovering digital assets, including technical and institutional constraints that are not fully reflected in the normative legal framework.

Thirdly, the proposed Integrated Digital Asset Recovery Framework (IDARF) remains conceptual and normative in nature. Although it has been developed through the synthesis of legal theory, comparative legal analysis, and an evaluation of the Financial Action Task Force (FATF) Recommendations and international best practices, the framework has not yet been tested within Indonesia's institutional context through pilot projects or policy simulations. Accordingly, the practical effectiveness of IDARF requires further validation through multidisciplinary research integrating legal scholarship, information technology, financial sector governance, and public policy.

These limitations provide valuable directions for future research. Subsequent studies should combine doctrinal legal analysis with empirical research to evaluate the implementation of digital asset recovery mechanisms within law enforcement agencies and financial regulatory institutions. Employing socio-legal or mixed-methods approaches would offer a more comprehensive understanding of the relationship between regulatory design, institutional capacity, and the practical effectiveness of law enforcement.

The rapid evolution of digital technology also raises a range of emerging legal issues that warrant further scholarly attention. These include the use of artificial intelligence in criminal investigations, the governance of public and private blockchain networks, the legal implications of Central Bank Digital Currencies (CBDCs) for asset recovery regimes, the regulation of decentralised finance (DeFi), procedures for the seizure and confiscation of non-fungible tokens (NFTs), and the governance of cross-border digital evidence. Further research into digital asset valuation methodologies, standards for managing seized cryptocurrency, and the protection of third-party rights would also make important contributions to the development of criminal procedure in the digital economy.

From a comparative law perspective, future research should examine the implementation of the Financial Action Task Force (FATF) Recommendations across jurisdictions representing different legal traditions in order to identify best practices that may be adapted to the Indonesian legal system. Such comparative analysis would provide a stronger empirical foundation for harmonising Indonesia's regulatory framework with the evolving international anti-money laundering and counter-terrorist financing regime.

The digital transformation of the global economy has fundamentally altered the nature of financial crime, shifting it from offences involving conventional assets to technologically enabled crimes operating through global networks and cross-border digital financial instruments. In this environment, the effectiveness of the criminal justice system can no longer be measured solely by its ability to prosecute and punish offenders, but also by the State's capacity to trace, freeze, seize, confiscate, and recover criminal assets efficiently, transparently, and in accordance with the principles of the Rule of Law.

Against this background, Indonesia's criminal law reform must move beyond fragmented, sector-specific regulation towards an integrated, adaptive, and technology-driven legal framework. The Integrated Digital Asset Recovery Framework (IDARF) developed in this study offers such a framework by bringing together Criminal Liability, Digital Asset Tracing, Blockchain Analytics, Beneficial Ownership Verification, compliance with the Financial Action Task Force (FATF) Recommendations, international cooperation, the protection of human rights, and the principles of Due Process of Law within a coherent legal model. Rather than replacing the existing legal framework, IDARF is intended to serve as a strategic blueprint for legal reform that strengthens the effectiveness of asset recovery, enhances the integrity of Indonesia's criminal justice system, and reinforces the country's legal resilience in responding to the evolving challenges of digital financial crime. Its implementation has the potential to establish a modern asset recovery regime that is responsive to technological innovation while remaining firmly grounded in the principles of justice, legal certainty, and sound global financial governance.

References

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in money laundering and fraud. *Journal of Money Laundering Control, 22*(2), 210–216.

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation, 6*(1), 45–62.

Basel Institute on Governance. (2024). *Basel AML Index 2024*. Basel Institute on Governance.

Bentham, J. (1996). *An introduction to the principles of morals and legislation*. Oxford University Press. (Original work published 1789).

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69*(2), 283–305.

Chohan, U. W. (2017). Cryptocurrencies and money laundering: Legal and regulatory issues. *Journal of Money Laundering Control, 20*(4), 396–406.

Dupuis, D., & Gleason, K. (2021). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime, 28*(1), 60–74.

Durner, T., & Shetret, L. (2015). Understanding bank de-risking and its effects on financial inclusion. *OCCASIONAL Journal of Financial Crime*, 22(3), 315–329.

Dworkin, R. (1986). *Law's empire*. Harvard University Press.

Egmont Group. (2021). *Egmont Group Annual Report 2021*. Egmont Group.

European Parliament & Council of the European Union. (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).*

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Europol.

Financial Action Task Force. (2021). *Second 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs*. FATF.

Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF.

Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.*

Financial Action Task Force. (2023). *Amendments to the FATF Standards to Strengthen Global Asset Recovery*. FATF.

Financial Action Task Force. (2023). *Guidance on Beneficial Ownership of Legal Persons*. FATF.

Financial Action Task Force. (2024). *The FATF Recommendations.*

Financial Action Task Force. (2024). *The FATF Recommendations*. FATF.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies, 32*(5), 1798–1853.

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

Fuller, L. L. (1969). *The morality of law* (Rev. ed.). Yale University Press.

Hart, H. L. A. (2012). *The concept of law* (3rd ed., P. Bulloch & J. Raz, Eds.). Oxford University Press.

Hendriyetty, N., & Grewal, B. (2017). Macroeconomics of money laundering: Effects and measurements. *Journal of Financial Crime, 24*(1), 65–81.

Houben, R., & Snyers, A. (2018). Cryptocurrency regulation and policy implications. *European Journal of Risk Regulation, 9*(4), 685–698.

International Monetary Fund. (2023). *Global Financial Stability Report*. IMF.

Kethineni, S., & Cao, Y. (2020). The rise in cryptocurrency crimes: Challenges for law enforcement. *International Journal of Cyber Criminology, 14*(1), 3–19.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*(1), 289–375.

MacCormick, N. (2007). *Institutions of law: An essay in legal theory*. Oxford University Press.

Marian, O. (2013). Are cryptocurrencies super tax havens? *Michigan Law Review First Impressions, 112*, 38–48.

Marzuki, P. M. (2021). *Penelitian hukum* (Edisi revisi). Kencana.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit Proceedings*, 1–14.

Organisation for Economic Co-operation and Development. (2023). *Global Forum on Transparency and Exchange of Information for Tax Purposes: Beneficial Ownership Implementation*. OECD Publishing.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity, 5*(1), 1–11.

Peraturan Bank Indonesia yang berkaitan dengan sistem pembayaran dan aset digital.

Peraturan Otoritas Jasa Keuangan mengenai perdagangan aset kripto dan inovasi teknologi sektor keuangan.

Peraturan Pusat Pelaporan dan Analisis Transaksi Keuangan mengenai pelaporan transaksi keuangan mencurigakan.

Posner, R. A. (2014). *Economic analysis of law* (9th ed.). Wolters Kluwer.

Pound, R. (1959). *Jurisprudence* (Vols. 1–5). West Publishing.

Ryder, N. (2012). Financial crime in the 21st century. *Journal of Financial Crime, 19*(4), 371–381.

Sunstein, C. R. (2018). *The cost-benefit revolution*. MIT Press.

Tamanaha, B. Z. (2004). *On the rule of law: History, politics, theory*. Cambridge University Press.

Teichmann, F. M. J. (2018). Recent trends in money laundering. *Journal of Financial Crime, 25*(2), 237–247.

Teichmann, F. M. J., & Falker, M. C. (2020). Money laundering through cryptocurrencies. *Journal of Money Laundering Control, 23*(2), 419–435.

Trautman, L. J. (2014). Virtual currencies; Bitcoin and what now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology, 20*(4), 1–108.

Umar, M., Polasik, M., & Wisniewski, T. P. (2021). Cryptocurrency regulation and financial crime prevention. *Journal of Financial Crime, 28*(4), 1081–1098.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

United Nations Office on Drugs and Crime. (2023). *World Drug Report 2023*. United Nations.

United Nations. (2000). *United Nations Convention against Transnational Organized Crime (Palermo Convention).*

United Nations. (2003). *United Nations Convention against Corruption (UNCAC).*

Van Hoecke, M. (Ed.). (2011). *Methodologies of legal research: Which kind of method for what kind of discipline?* Hart Publishing.

World Bank & United Nations Office on Drugs and Crime. (2007). *Stolen Asset Recovery (StAR) Initiative: Challenges, Opportunities, and Action Plan*. World Bank.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. (2020). Decentralized finance (DeFi). *Journal of Financial Regulation, 6*(2), 172–203.