Realism: Law Review
Volume 4 Nomor 1
April 2026

Legal Reconstruction of Digital Asset Confiscation of Cybercrime in Indonesia

P Pebrin Putra Yasa[1]

[1]Kepolisian Resor Jember, Indonesia, ppebrin@gmail.com
Corresponding Author: ppebrin@gmail.com

Abstract

This article examines the legal framework for digital asset confiscation in cybercrime within the Indonesian legal system. The rapid development of blockchain-based assets such as cryptocurrencies has created significant challenges in asset recovery, particularly due to their decentralized, pseudonymous, and borderless nature. This study employs a normative juridical method with legislative, conceptual, and comparative approaches. The findings reveal substantial legal, technical, and institutional limitations in identifying, tracing, and confiscating digital assets under existing regulations, including the Criminal Code and the ITE Law. This article proposes a hybrid legal reconstruction model integrating digital asset sovereignty, constructive seizure, and coercive key disclosure as mechanisms to strengthen digital asset confiscation in cybercrime cases. Additionally, this study incorporates a human rights perspective, emphasizing the protection of privacy rights, due process, and digital property rights in enforcement practices. This research contributes to the development of cyber law by offering a comprehensive and adaptive legal framework that integrates normative, technological, and institutional approaches to asset recovery in the digital era.

Keywords: *Cybercrime; Digital Asset Confiscation; Cryptocurrency Regulation; Blockchain Forensics; Asset Recovery*

A. INTRODUCTION

The rapid development of information technology has fundamentally transformed the nature of crime, shifting from conventional forms to complex cybercrime involving digital assets such as cryptocurrencies. However, the Indonesian criminal law framework remains rooted in a conventional paradigm that prioritizes tangible objects as the primary subject of regulation. This orientation reflects a normative limitation in addressing crimes involving

intangible assets, particularly in the context of asset confiscation. The decentralized nature of digital assets, their pseudonymity, and their reliance on blockchain systems create significant challenges in identification, tracing, and enforcement, which cannot be adequately resolved through existing legal mechanisms. This condition indicates a clear gap between technological developments and the readiness of national law, further compounded by limitations in institutional capacity, technological understanding, and enforcement infrastructure.

The development of information technology has brought fundamental changes to various aspects of life, including the patterns and nature of crime. Crimes that were previously conventional have now transformed into technology-based crimes, or cybercrimes, which are more complex. Cybercrime not only attacks information systems but also involves the use of digital technology as both a means and an object of crime, thus requiring a more adaptive and progressive legal approach (Adriani, 2020).

This study argues that the core issue lies in the outdated normative design of asset confiscation law, which fails to accommodate the characteristics of digital assets as objects of criminal law. Accordingly, this research offers a novel legal reconstruction model grounded in three key concepts: digital asset sovereignty, constructive seizure, and coercive key disclosure. These concepts are positioned as a normative critique and reorientation of the existing legal framework, shifting from a material-based approach toward a control and value-based paradigm. By integrating legal reform with technological enforcement mechanisms, this study not only identifies regulatory and practical obstacles but

also provides an adaptive and operational framework for strengthening digital asset confiscation within the Indonesian criminal justice system.

As cybercrime evolves, it is no longer limited to violations of computer systems but has expanded into the digital economy, particularly through the use of digital assets such as cryptocurrencies. These assets facilitate cross-border transactions without going through conventional financial authorities, making them often used as instruments in various crimes such as money laundering, fraud, and ransomware (Ali & Ridwan, 2020).

The decentralized nature of digital assets, independent of central authorities, makes them difficult for the state to control. Furthermore, the blockchain system used in cryptocurrency transactions allows for user anonymity or pseudonymity, making it difficult for law enforcement to identify perpetrators. This situation further complicates the law enforcement process in the context of cybercrime.

In the context of Indonesian law, cybercrime regulations still face various limitations, both normative and implementative. Existing regulations have not fully accommodated the development of digital technology, particularly regarding the regulation of digital assets as legal objects. This creates a gap between technological developments and the preparedness of the national legal system.

Furthermore, in law enforcement practice, the main problem faced is the aspect of proving and tracking digital transactions. Cryptocurrency-based transactions have characteristics that are difficult to trace conventionally, thus posing unique challenges in the process of proving criminal acts, particularly in cases of digital-based money laundering (Ilmi & Lubis, 2025).

Furthermore, previous research shows that most studies on cybercrime still focus on general regulatory and preventive aspects, without in-depth examination of the mechanisms for confiscating digital assets. For example, Putri and Fauzy's (2023) study focused more on proving cyberlaundering crimes through NFTs, while other studies focused more on the legality of cryptocurrency within the Indonesian legal system (Thistanti et al., 2022).

On the other hand, recent developments indicate that the use of cryptocurrency in the criminal ecosystem is increasing, creating a significant legal vacuum in the Indonesian criminal justice system. This is evident in the lack of clear regulations regarding criminal liability and mechanisms for handling digital assets as proceeds of crime (Pambudi & Fakrulloh, 2025).

Furthermore, challenges in cybercrime law enforcement are not only normative but also related to institutional aspects and the capacity of law enforcement officials. Limited technological understanding and the lack of supporting infrastructure hinder optimal law enforcement against digital-based crimes (Hasri et al., 2025).

Based on this description, it can be concluded that there is a significant gap between the development of digital technology and the readiness of national law to regulate digital asset confiscation. Therefore, this research is crucial to analyze existing legal regulations, identify obstacles encountered, and formulate a legal reconstruction of digital asset confiscation within the Indonesian criminal justice system.

In line with the issues identified above, this study is structured around three main problem formulations. First, it examines the legal regulations on asset

confiscation within the Indonesian legal system, focusing on the existing normative framework and its limitations. Second, it analyzes the characteristics of digital assets and the various constraints encountered in their confiscation, including technical, juridical, and jurisdictional challenges. Third, it formulates a reconstruction model of digital asset confiscation law that is adaptive to technological developments and capable of supporting effective law enforcement within the Indonesian criminal justice system.

This study offers a distinct contribution by developing a novel legal reconstruction model that integrates three key concepts: digital asset sovereignty, constructive seizure, and coercive key disclosure. Unlike prior studies that primarily focus on regulatory gaps or the legality of cryptocurrencies, this research proposes a hybrid framework that combines legal reform with technological enforcement mechanisms. This approach not only expands the scope of criminal law but also enhances its operational capacity in addressing cybercrime involving digital assets.

B. RESEARCH METHOD

This research is a normative legal study with a legislative, conceptual, and comparative approach. Primary legal materials consist of laws and regulations related to cybercrime and asset forfeiture, while secondary legal materials include relevant books and scientific journals (Zainuddin, 2022). The legal materials were collected through literature review, while analysis was conducted qualitatively with a prescriptive approach to formulate an ideal legal concept. This research approach is implemented through an analysis of relevant laws and regulations to identify gaps, conflicts, and unclear norms in the

regulation of cybercrime and digital asset forfeiture. This is then deepened through a conceptual approach to reconstruct the understanding of ownership and control of blockchain-based assets in criminal law. Furthermore, a comparative approach is used to compare legal practices in Indonesia with other jurisdictions that are more advanced in regulating digital assets, thus obtaining an overview of best practices that can be adapted. All legal materials are analyzed qualitatively through a comprehensive legal interpretation method, with the ultimate goal of formulating a prescriptive, ideal, and applicable legal concept to address the challenges of digital asset forfeiture in the cybercrime era. Furthermore, the conceptual approach is utilized to reconstruct the legal understanding of ownership and control over blockchain-based digital assets within the framework of criminal law, particularly in relation to asset confiscation. The comparative approach is employed to compare Indonesia's legal framework with jurisdictions that have more advanced regulations on digital assets, thereby identifying best practices that can be adapted into the national system. Through a comprehensive legal interpretation method, this study aims to identify normative gaps, inconsistencies, and ambiguities, and ultimately to formulate a prescriptive, coherent, and applicable model for digital asset forfeiture in addressing the challenges of cybercrime in the digital era.

C. RESULT AND DISCUSSION

1. Legal Regulations on Asset Confiscation in the Indonesian Legal System

The regulation of asset forfeiture in Indonesian criminal law is traditionally rooted in the concept of tangible objects. In the classical

paradigm, objects subject to seizure and confiscation are those that have a physical existence and are within the territorial jurisdiction of the state. This concept becomes problematic when faced with digital assets, which are non-physical and globally distributed.

In practice, there are no explicit regulations recognizing digital assets as objects of forfeiture in criminal law. This creates legal uncertainty and limits law enforcement against cybercrime. However, in global developments, digital assets have become an integral part of the criminal ecosystem, particularly in the context of money laundering and illicit financing (Cahyani, 2019).

Current regulations in Indonesia, particularly Law Number 1 of 2023 concerning the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (the ITE Law), have not been designed to accommodate the unique characteristics of blockchain-based assets. The Indonesian Criminal Code, as a general criminal law, still focuses on tangible property, as reflected in the provisions concerning theft in Article 476 of the Criminal Code, which require "goods" as the object of the crime. The interpretation of "goods" in Indonesian criminal law practice tends to be limited to physical objects or those that can be directly controlled, thus giving rise to debate when related to digital assets such as cryptocurrencies, which are non-physical, decentralized, and network-based. Consequently, the application of the Criminal Code norms to crimes involving blockchain-based assets often faces conceptual and interpretive limitations.

Article 476 of Law Number 1 of 2023 concerning the Criminal Code (KUHP) reflects a classical construction of theft that presupposes “goods” as the object of the crime. Doctrinally, this provision is rooted in a material-based paradigm, where the element of barang is generally interpreted as a tangible object that can be physically possessed, transferred, or controlled. This interpretation is reinforced by the traditional requirement of “taking”, which implies a physical act of moving an object from the control of another person. Within this framework, the legal meaning of possession (bezit) and control remains closely tied to physical dominion, thereby limiting the scope of the provision to conventional forms of property. As a result, the normative structure of Article 476 KUHP demonstrates a conceptual rigidity that does not readily extend to non-physical assets.

When applied to blockchain-based digital assets such as cryptocurrencies, this provision encounters significant interpretive challenges. Digital assets do not exist in a physical form and are not “taken” in the conventional sense, but rather accessed or transferred through cryptographic keys within a decentralized network. The absence of physicality and the reliance on private key control undermine the applicability of the traditional elements of barang and mengambil, creating a legal ambiguity in qualifying such conduct as theft under the Criminal Code. Consequently, the current formulation of Article 476 KUHP reveals a normative gap, as it fails to capture the reality of control-based ownership inherent in digital assets. This limitation highlights the need for a reconceptualization of the object of theft from a material-based approach toward a control- and value-based paradigm that is more compatible

with the characteristics of blockchain technology.

Meanwhile, the Electronic Information and Transactions (ITE) Law has indeed expanded the scope of legal objects by recognizing electronic information and/or electronic documents as protected objects, as stipulated in Article 5 paragraph (1) and Article 6 of the ITE Law. Furthermore, the criminal provisions in Articles 30, 32, and 35 of the ITE Law provide a legal basis for illegal access, manipulation, and destruction of electronic systems. However, these norms focus more on system and data protection, rather than on regulating the status or mechanisms for confiscation of digital assets resulting from criminal acts. In other words, although the ITE Law accommodates the digital dimension, this regulation does not comprehensively address the specific characteristics of blockchain-based assets, such as private key-based ownership, cross-jurisdictional transactions, and decentralized nature. Consequently, a legal vacuum remains in the context of law enforcement regarding digital assets.

The Electronic Information and Transactions Law (ITE Law) represents a significant normative expansion by recognizing electronic information and/or electronic documents as legal objects, as stipulated in Article 5 paragraph (1) and Article 6. This recognition marks a departure from the strictly material-based paradigm found in the Criminal Code, as it acknowledges the legal validity and evidentiary value of intangible digital data. Furthermore, Articles 30, 32, and 35 establish criminal liability for unauthorized access, data manipulation, and interference with electronic systems, thereby providing a legal framework to address cyber-related misconduct. However, a closer

doctrinal analysis shows that these provisions are primarily designed to protect the integrity, confidentiality, and availability of electronic systems and data, rather than to regulate digital assets as objects of economic value subject to criminal confiscation.

This normative orientation creates a structural limitation when applied to blockchain-based digital assets. While the ITE Law can criminalize unauthorized access to a crypto wallet or manipulation of digital data, it does not provide a clear legal basis for identifying, seizing, or confiscating the digital assets themselves as proceeds of crime. The absence of provisions addressing private key control, decentralized transaction systems, and cross-border asset mobility results in a regulatory gap between system protection and asset recovery. Consequently, although the ITE Law accommodates the digital dimension at the level of data and systems, it fails to construct a coherent legal regime for digital asset confiscation, thereby leaving a significant vacuum in the Indonesian criminal justice system in responding to asset-based cybercrime.

The reconstruction of digital asset confiscation must be aligned with fundamental human rights principles. The implementation of mechanisms such as coercive key disclosure raises critical concerns regarding the right against self-incrimination and the protection of privacy. Forcing individuals to disclose private keys may violate due process guarantees if not conducted under strict judicial authorization and procedural safeguards.

Furthermore, digital assets must be recognized as part of digital property rights, which are protected under both constitutional principles and

international human rights frameworks. Arbitrary seizure or restriction of access without clear legal basis risks undermining legal certainty and public trust in the justice system.

Therefore, a balance must be established between effective law enforcement and the protection of individual rights. The principle of proportionality must guide any enforcement action involving digital assets. Legal mechanisms such as constructive seizure and blockchain-based monitoring must be accompanied by accountability, transparency, and judicial oversight.

In this context, this study emphasizes a rights-based approach to digital asset confiscation, ensuring that the expansion of state authority in cyberspace does not lead to excessive or abusive enforcement practices.

The absence of a clear regulatory framework demonstrates that the Indonesian legal system has yet to keep pace with rapid advancements in digital technology. Consequently, a comprehensive legal reform is required to accommodate the unique characteristics of digital assets as objects within criminal law. From a contemporary criminal law perspective, the concept of asset confiscation has shifted from a purely material-based approach toward one that prioritizes the economic value of assets. Although digital assets lack physical form, they possess substantial economic significance and are actively traded within the global financial ecosystem. Accordingly, restricting confiscation solely to tangible objects reflects an outdated legal approach that is no longer aligned with current technological and economic developments (Primadhany, et al, 2025).

Furthermore, in the context of cybercrime, digital assets are often used as a means to conceal the proceeds of crime. Perpetrators utilize blockchain technology to move and disguise the flow of funds quickly and across jurisdictions. This makes it difficult for law enforcement officials to track and freeze assets, thus compromising the effectiveness of law enforcement (Ilmi & Lubis, 2025).

From a criminal law policy perspective, this situation demonstrates the urgent need to expand the concept of "objects" in criminal law to include digital assets. This expansion is not merely terminological but must also be accompanied by technical regulations that enable law enforcement officials to effectively take legal action against these assets (Sitanggang et al., 2024).

On the other hand, international developments indicate that various countries have begun to adopt a more progressive approach to handling digital assets. Several jurisdictions have recognized cryptocurrency as property subject to seizure and forfeiture in criminal proceedings. This approach demonstrates a paradigm shift from conventional law to one that adapts to technological developments.

However, the implementation of digital asset forfeiture faces not only normative challenges but also complex technical challenges. One major obstacle is the need for technical expertise in blockchain analysis, which not all law enforcement officers possess. Without adequate technological support, digital asset forfeiture efforts will be difficult to implement effectively.

Furthermore, jurisdictional issues are also crucial in handling digital assets. Digital asset transactions can occur across borders without going

through the formal financial system, creating difficulties in determining applicable laws and competent authorities. This situation demands more intensive international cooperation in law enforcement against cybercrime.

Thus, it can be concluded that the problem of digital asset forfeiture is not only related to a lack of norms but also concerns technical and institutional complexities. Therefore, the legal reformulation carried out must be comprehensive, covering normative, technical, and institutional aspects, in order to be able to answer the challenges of cybercrime in the digital era effectively and sustainably (Cahyani, 2019).

2. Characteristics of Digital Assets and Constraints to Confiscation

Digital assets have characteristics that are fundamentally different from conventional assets. First, their decentralized nature means there is no central authority that can control or freeze assets. Second, pseudonymity allows the identity of asset owners to be obscured through digital addresses. Third, control over assets relies entirely on private keys (Stevani & Disemadi, 2021).

These characteristics create various obstacles in the asset confiscation process. Technically, transaction tracking requires complex blockchain analysis capabilities. Legally, there are challenges in determining legal jurisdiction, given that transactions can occur across countries without geographical boundaries.

Furthermore, without access to private keys, law enforcement officials lack control over digital assets. This differs from conventional assets, which can be physically seized. Therefore, existing legal mechanisms are inadequate to address these challenges.

The decentralized nature of digital assets fundamentally shifts the paradigm of legal control from institution-based to protocol-based. In conventional financial systems, the state can intervene through banking institutions or financial authorities as "gatekeepers." However, in blockchain systems, there is no central entity with the authority to freeze or control assets. This system operates through a distributed network validated by global consensus, significantly limiting state intervention (Thistanti et al., 2022).

The legal implication of this situation is a "displacement of authority," where the state's power to enforce the law is no longer absolute over the subject of a crime. The state cannot unilaterally order the freezing of assets as in the conventional banking system. This creates serious challenges in implementing the principle of legal sovereignty, particularly in the context of criminal law enforcement against cross-border crimes (Ali & Ridwan, 2020).

Furthermore, the concept of pseudonymity in blockchain creates its own complexities in legal evidence. Although every transaction is transparently recorded on the blockchain, the perpetrator's identity is not directly linked to their real-world identity. Users are identified only through alphanumeric wallet addresses, requiring advanced analytical techniques to link digital activity to specific legal entities. This situation makes the process of proof in criminal law more complex than for conventional crimes.

Furthermore, pseudonymity does not guarantee absolute anonymity, but rather creates "traceable anonymity," a condition in which transactions can be traced but identities remain hidden. This opens up space for new approaches to law enforcement through blockchain forensics. However, this approach

requires high-tech capabilities and cross-platform data integration, which law enforcement officials in many developing countries do not yet fully possess.

From a technical perspective, reliance on private keys as the sole means of controlling digital assets presents a crucial problem. Private keys are exclusive and cannot be recovered by third parties. Therefore, even if law enforcement officials successfully identify the location of assets on the blockchain, without access to the private keys, those assets cannot practically be seized or transferred. This demonstrates the gap between identification capabilities and asset control capabilities in the current legal system.

This situation creates a dilemma in criminal law, particularly regarding the effectiveness of asset confiscation sanctions. In a conventional context, asset confiscation is a crucial instrument for breaking the profit chain of criminal acts. However, in the context of digital assets, the effectiveness of these instruments is questionable due to technical barriers that cannot be overcome through a normative approach alone. In other words, criminal law faces structural limitations in addressing technology-based crimes (Sitanggang et al., 2024).

Further complicating matters, the development of cross-chain blockchain technology further complicates the process of asset tracking and confiscation. This technology allows the movement of assets between blockchains without going through mechanisms easily monitored by authorities. As a result, criminals can quickly move assets across multiple networks to evade tracking, thereby weakening the effectiveness of law enforcement (Putri & Fauzy, 2023).

3. Reconstruction of Digital Asset Confiscation Law

Reconstructing the law on digital asset forfeiture cannot be achieved simply by expanding existing norms, but rather requires a fundamental shift in the legal paradigm. Conventional criminal law is based on the assumption that the object of the crime is within the territorial control of the state, while digital assets exist in cyberspace, which recognizes no geographical boundaries. Therefore, an extraterritorial and network-based legal approach is required to reach the object of the crime (Pambudi & Fakrulloh, 2025).

Table 1
Comparison of Virtual Asset Regulatory Frameworks (US, EU, FATF) and Their Relevance for Indonesia

Aspect	United States	European Union	FATF
Appraoch	Law + technology	AML & KYC regulation	Global standards
Asset Status	Recognized as property	Recognized in financial system	Recognized as virtual assets
Enforcement	Blockchain analytics	KYC & reporting	Transparency & reporting
Strengths	Effective asset tracing	Integrated & harmonized system	International benchmark
Weakness	High technological dependency	Complex coordination	Uneven implementation
Relevance for Indonesia	Need to adopt blockchain forensic technology	Need for AML integration and cross-agency coordination	Gradual adaptation is needed according to national capacity.

Source: personal data processing, (2026)

In practice in the United States, the approach to digital asset forfeiture has evolved through the integration of criminal law and digital investigative technology. Law enforcement authorities rely not only on legal norms but also utilize blockchain analytics tools to trace the flow of funds in real time. This approach demonstrates that the effectiveness of digital asset forfeiture

depends heavily on the state's ability to simultaneously combine normative and technical aspects (William & Urbanisasi, 2025).

Furthermore, the legal system in the United States has recognized cryptocurrency as a form of property subject to seizure and confiscation. This recognition provides a strong legal basis for law enforcement officials to take repressive action against digital assets linked to criminal acts. This eliminates the regulatory gap that hinders the asset recovery process (Smith, 2022).

In the European Union, the approach tends to be more comprehensive, integrating anti-money laundering (AML) regulations into digital asset oversight. These regulations require crypto asset service providers to implement know-your-customer (KYC) principles, thus facilitating the identification of perpetrators in digital transactions. This approach strengthens both the preventive and repressive aspects of handling cybercrime (Maulana, E.T., 2024).

Furthermore, the European Union also emphasizes the importance of legal harmonization between member states in addressing cybercrime. Given its cross-border nature, regulatory disparities can create loopholes exploited by criminals. Therefore, regulatory coordination is key to effective law enforcement at the regional level (Maulana, E.T., 2024).

Meanwhile, international organizations such as the Financial Action Task Force (FATF) have issued global standards regarding digital asset oversight. The FATF emphasizes the importance of transaction transparency and reporting obligations for entities involved in the crypto ecosystem. These standards serve as a reference for many countries in formulating legal policies

related to digital assets (Maulana, E.T., 2024).

However, the implementation of these international standards is not always effective in all countries. Developing countries, including Indonesia, often face limitations in technological infrastructure and human resources. Consequently, there is a gap between global standards and national practices in law enforcement against cybercrime.

Beyond technical factors, there are also challenges in the political aspects of national law. Each country has different interests and priorities in regulating digital assets, so not all international standards can be adopted directly. Therefore, an adaptive approach is needed that takes into account the social, economic, and legal conditions of each country (Putri & Fauzy, 2023).

In the Indonesian context, the adoption of international models must be undertaken selectively and adapted to domestic conditions. Mechanisms applied in developed jurisdictions cannot be transplanted directly without contextual adjustments. For instance, the implementation of blockchain forensic technologies demands substantial financial resources, advanced technical infrastructure, and enhanced capacity building for law enforcement agencies (Arifin, Z., & Handayani, E. P, 2024).

Furthermore, Indonesia needs to develop a hybrid model that combines normative and technical approaches to handling digital assets. This approach focuses not only on establishing regulations but also on strengthening institutional and technological capacity. Thus, the legal system developed will not only be formal but also operational and effective in practice (Pambudi & Fakrulloh, 2025).

Ultimately, lessons learned from international practice demonstrate that successful digital asset confiscation cannot be achieved through a single approach. An integration of clear regulations, adequate technology, and effective international cooperation is required. Without these three elements, law enforcement efforts against cybercrime will always face structural limitations that are difficult to overcome.

In this context, a novelty that can be offered is the concept of "digital asset sovereignty," an approach that positions the state not merely as a territorial authority but also as an actor with the legitimacy to access and control digital assets through specific legal mechanisms. This concept extends the scope of state sovereignty into cyberspace without relying solely on physical territorial boundaries (Hasri et al., 2025).

Furthermore, legal reconstruction must also accommodate an access control-based approach rather than simply formal ownership. In blockchain systems, control over assets is determined by who has access to the private key, not by who is legally recognized as the owner. Therefore, criminal law needs to adopt the concept of "effective control" as the basis for determining objects of confiscation (Thistanti et al., 2022).

Another novelty lies in the development of a coercive key disclosure mechanism, which is the legal authority for law enforcement officials to compel perpetrators to hand over private keys under certain conditions. Although this concept has sparked debate regarding privacy rights and the principle of non-self-incrimination, this approach is beginning to be considered as a solution to address the technical limitations of digital asset

confiscation.

Furthermore, regulations are needed regarding constructive seizure, a concept of confiscation that does not always take the form of physical control, but can also involve restricting access to or controlling digital assets. In this context, confiscation can be carried out by blocking access to certain platforms or collaborating with crypto service providers to restrict transactions (Stevani & Disemadi, 2021).

In a more progressive dimension, legal reconstruction could also lead to the establishment of state-controlled digital wallets, namely digital wallets managed by the state to hold seized assets. This mechanism would enable the state not only to confiscate but also to manage digital assets transparently and accountably as part of an asset recovery system.

Another novelty is the integration of criminal law and technology through a blockchain-based enforcement approach. In this model, law enforcement is not only carried out externally to the blockchain system but also through the integration of legal mechanisms into the technological system itself. For example, through smart contracts that can automatically restrict or freeze assets based on legal orders.

The proposed reconstruction model is structured as a three-layer framework that integrates normative, procedural, and institutional dimensions in addressing digital asset confiscation. At the normative level, the legislature must explicitly recognize digital assets as objects of confiscation based on their economic value rather than their physical form. This shift reflects the evolution of criminal law from a material-based paradigm to a value-based

approach, where intangible assets such as cryptocurrencies are treated as legally protected property. Several studies have emphasized that the absence of legal recognition of digital assets creates a significant barrier to effective law enforcement, particularly in cybercrime and money laundering cases involving blockchain-based transactions (Kethineni & Cao, 2020; Levi & Soudijn, 2020). Therefore, reformulating the legal definition of confiscable assets is a fundamental prerequisite for adapting criminal law to the digital economy.

At the procedural level, the legal system must regulate innovative mechanisms such as constructive seizure and coercive key disclosure to address the technical barriers inherent in digital asset control. Constructive seizure allows authorities to exercise control over assets without requiring physical possession, which is particularly relevant in decentralized blockchain systems. Meanwhile, coercive key disclosure provides a legal basis for compelling suspects to grant access to private keys under strict judicial supervision. However, these mechanisms must be carefully designed to balance enforcement effectiveness with the protection of fundamental rights, particularly the right against self-incrimination and the right to privacy. Empirical and doctrinal studies highlight that the integration of blockchain forensic tools and procedural safeguards is essential to ensure both the traceability of transactions and the legitimacy of law enforcement actions (Möser et al., 2021).

At the institutional level, effective implementation requires the establishment of a specialized cyber asset task force that integrates legal,

financial, and technological expertise. The complexity of digital asset tracing and confiscation demands interdisciplinary coordination among law enforcement agencies, financial intelligence units, and technology experts. International experience demonstrates that jurisdictions with dedicated units and advanced analytical capabilities are more successful in recovering illicit digital assets and disrupting criminal networks (Europol, 2023). This multi-layered approach ensures that legal reform is not merely symbolic but operational and enforceable in practice, enabling the criminal justice system to respond more effectively to the evolving challenges of cybercrime in the digital era.

Furthermore, legal reconstruction also needs to accommodate the concept of predictive asset recovery, namely the use of artificial intelligence to predict the movement of digital assets resulting from crime. This approach allows law enforcement officials to act preemptively before assets are transferred to hard-to-reach jurisdictions.

In an institutional context, innovation can be realized through the formation of a hybrid cyber asset task force, a cross-sectoral unit combining legal, technological, and financial expertise. This model differs from conventional, sector-based approaches and is therefore more adaptable to the complexity of cybercrime (Hardiago et al., 2025).

Furthermore, a multi-layered jurisdiction-based approach is needed, where jurisdiction is determined not only by the location of the perpetrator or victim, but also by the location of the blockchain nodes, exchanges, and servers involved in the transaction. This approach provides flexibility for

countries in enforcing laws against cross-border cybercrime.

Another significant innovation is the development of a legal interoperability framework, a mechanism that allows national legal systems to interact with the legal systems of other countries in handling digital assets. This is crucial given the global nature of blockchain, which cannot be regulated unilaterally by a single country (Hardiago et al., 2025).

Ultimately, the reconstruction of digital asset forfeiture law must be understood as a holistic process of legal system transformation. Simply updating regulations is not enough; it must also encompass changes in paradigms, institutions, and technology. The novelty offered in this research lies in the integration of these three aspects into a coherent conceptual framework, enabling it to address cybercrime challenges more effectively and sustainably.

D. CONCLUSION

The current legal framework in Indonesia remains rooted in a conventional paradigm that limits asset forfeiture to tangible objects, resulting in a significant normative gap in addressing cybercrime involving digital assets. The decentralized structure, pseudonymity, and private key-based control of digital assets create complex legal and technical challenges that cannot be resolved through existing mechanisms. Consequently, asset recovery efforts remain ineffective in dealing with technology-based crimes, indicating that the national legal system has not yet adapted to the evolution of digital technology.

The legislature and government must address these challenges by undertaking a comprehensive legal reconstruction that shifts the paradigm from

formal ownership to effective control and explicitly recognizes digital assets as objects of criminal law. They must operationalize this reconstruction through concrete measures, including: (i) revising the Criminal Code and related laws to formally recognize digital assets; (ii) regulating coercive key disclosure mechanisms under strict judicial authorization; and (iii) adopting blockchain forensic technologies supported by standard operating procedures for tracing, freezing, and managing digital assets, including the establishment of state-controlled digital wallets. Law enforcement institutions must also strengthen their capacity by establishing a specialized cyber asset task force to ensure effective implementation.

This study advances a theoretical model of digital asset forfeiture grounded in an integrated framework that combines international legal harmonization and a human rights-based approach. Within this model, the state acts as a coordinating authority that strengthens cross-border cooperation through mutual legal assistance mechanisms while aligning domestic regulations with global standards, particularly those developed by the Financial Action Task Force, reflecting the principle of transnational legal integration necessary to address the borderless nature of cybercrime. At the same time, this model incorporates a rights-based normative constraint, ensuring that enforcement mechanisms operate within the protection of fundamental rights, including privacy, due process, and digital property rights. This dual structure integrating transnational enforcement capacity with constitutional safeguards forms a balanced theoretical paradigm that repositions digital asset forfeiture from a purely repressive instrument into a regulated, accountable, and adaptive legal process capable of

guiding legislative reform, institutional design, and law enforcement practices in the digital age.

REFERENCES

Adriani, W. (2020). *Cyberlaw: Aspek Hukum Teknologi Informasi*. Jakarta: PT. Citra Aditya Bakti.

Ali, M., & Ridwan, R. (2020). *Cyber Law: Aspek Hukum Teknologi Informasi*. Jakarta: RajaGrafindo Persada.

Ali, Zainuddin. (2022). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Cahyani, E. (2019). *Hukum Pidana Siber di Indonesia*. Bandung: Refika Aditama.

David Hardiago, et al. (2025). *Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law*. Indonesian Journal of Criminal Law Studies, 10(1), pp. 297–340. doi:10.15294/ijcls.v10i1.22557.

Europol. (2023). Crypto-assets: Tracing the evolution of criminal finances.

Hasirudin Hasri , et. al. (2025). *Kejahatan Cybercrime Dan Penanggulangannya Dalam Kerangka Sistem Hukum Nasional*. Indonesian Journal of Legality of Law, 7(2), pp. 281–287. doi:10.35965/ijlf.v7i2.6240.

Arifin, Z., & Handayani, E. P. (2024). *Cybercrime: Menyelisik penegakan hukum dan penanggulangannya*. Yogyakarta: Deepublish.

Maulana, E.T. (2024) 'Regulasi Travel Rule terhadap transaksi aset virtual lintas batas dalam konteks Decentralized Finance di Indonesia: Studi banding terhadap Markets in Crypto-Assets (MiCA) di Uni Eropa', Jurnal Rectum, 6(3), pp. 565–584. doi: http://dx.doi.org/10.46930/jurnalrectum.v6i3.5013

Möser, M., Böhme, R., & Breuker, D. (2021). An empirical analysis of traceability in the Bitcoin network. Journal of Cybersecurity, 7(1), 1–17.

Musfiratul Ilmi and Putri Mei Lestari Lubis. (2025). *Tantangan Pembuktian Tindak Pidana Pencucian Uang Melalui Cryptocurrency Dalam Sistem Hukum Pidana Indonesia.* El-iqtishady: Hukum Ekonomi Syariah 7(1), pp. 448-455 doi: https://doi.org/10.24252/el-iqthisady.v7i1.57409.

Pambudi Pambudi and Zudan Arief Fakrulloh (2025) *Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, and Legal Voids in the Criminal Law System in Indonesia*. Majelis: Jurnal Hukum Indonesia, 2(3), pp. 105–125. doi: 10.62383/majelis.v2i3.1042.

Primadhany, E. F.,et al. (2025). *Pengantar hukum siber Indonesia*. Sada Kurnia Pustaka.

Raden Roro Fara Anissa Putri and Elfian Fauzy (2023). *Upaya Hukum Pembuktian Tindak Pidana Cyber Laundering yang Dilakukan Melalui Non-Fungible Token (NFT).* Lex Renaissance, 7(4), pp. 836–851. doi: 10.20885/JLR.vol7.iss4.art10.

Sitanggang, A. S., Darmawan, F. dan Saputra, D. 2024. *Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber*. Jurnal Pendidikan dan Teknologi Indonesia, 4(3), hlm. 79-83. doi: 10.52436/1.jpti.409.

Thistanti, I. A. S. C., Sugiartha, I. N. G. . and Arthanaya, I. W. 2022. *Kajian Yuridis Mengenai Legalitas Cryptocurrency di Indonesia*. Jurnal Preferensi Hukum, 3(1), pp. 7–11. Available at: https://ejournal.warmadewa.ac.id/index.php/juprehum/article/view/4592

Wardani, A., Ali, M. ., & Barkhuizen, J. . (2022). Money Laundering through

Cryptocurrency and Its Arrangements in Money Laundering Act. Lex Publica, 9(2), 49–66. https://doi.org/10.58829/lp.9.2.2022.49-66

William, J., & Urbanisasi, U. (2025). *Analisis Yuridis terhadap Kedudukan Cryptocurrency sebagai Objek Hukum dalam Hukum Perdata Indonesia*. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(2), 4657–4662. https://doi.org/10.31004/riggs.v4i2.1300

Winnie Stevani and Hari Sutra Disemadi. (2021). *Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime*. Hang Tuah Law Journal, 5(1), pp. 52–66. doi: 10.30649/htlj.v5i1.32.