

CONFISCATION OF CRYPTO ASSET EVIDENCE: LEGAL CHALLENGES IN CYBERCRIME ENFORCEMENT IN INDONESIA

I Gede Widhartama^{[1]*}; Wulanmas Frederik^[2]; Merry Elizabeth Kalalo^[3]; Herlianty Y.A. Bawole^[4]

Doktoral Fakultas Hukum Universitas Sam Ratulangi

Bahu Village, Malalayang Subdistrict, Manado City, North Sulawesi Province, Indonesia

*Email: gede.widhartama@gmail.com

* Corresponding Author

Citation: Widhartama, I. G., *et al.* 2025. Confiscation of Crypto Asset Evidence: Legal Challenges in Cybercrime Enforcement in Indonesia, *International Journal of Law, Environment, and Natural Resources (INJURENS)*, 5 (2), 157-172.

Academic Editor: Nurmaya Safitri

Publisher's Note: Scholar Center stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright:

© 2025 by the authors. Submitted for open access publication in International Journal of Law, Environment, and Natural Resources (INJURENS) under the terms and conditions of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 license (CC BY NC SA 4.0). For more information visit (<http://creativecommons.org>).

Abstract: *The development of information technology has introduced crypto assets as an innovation in the global financial system. The emergence of crypto assets presents both opportunities and challenges, particularly in the enforcement of cybercrime law in Indonesia. Their decentralized, anonymous, and cross-border nature makes them difficult to trace and highly vulnerable to misuse for crimes such as money laundering, online fraud, and terrorism financing. Within the national legal framework, regulatory ambivalence persists: Bank Indonesia prohibits the use of crypto as a means of payment, while Bappebti legitimizes it as a futures commodity. This dualism creates complex legal challenges, especially when crypto assets are treated as evidence in criminal proceedings. The Criminal Procedure Code (KUHP), which remains oriented toward conventional evidence, has not accommodated the unique characteristics of digital assets, resulting in the seizure and confiscation of crypto assets through broad interpretations that often invite conflicting views and pretrial disputes. This research adopts a normative-empirical juridical approach using a statute approach, supported by secondary data and interviews. The findings reveal that the regulation of crypto asset confiscation in Indonesia remains fragmented, spread across multiple legal instruments, and lacks explicit technical guidance. Consequently, weaknesses persist in legal certainty, procedural effectiveness, third-party protection, and Indonesia's alignment with international standards. Therefore, this article recommends establishing comprehensive digital asset confiscation regulations, enhancing law enforcement technical capacity, clarifying institutional authority, and integrating national mechanisms with international standards such as the FATF and the Budapest Convention to ensure effective and legally certain implementation consistent with the rule of law.*

Keywords: *Crypto Assets; Evidence; Confiscation; Cyber Crime; Legal Certainty.*

1. INTRODUCTION

Advances in information technology have drastically transformed the global financial system. Over the past decade, one of the most significant innovations has

been the emergence of crypto assets, beginning with Bitcoin in 2009, which have now grown to thousands of types with total market capitalizations reaching trillions of dollars (Nakamoto, 2008). Blockchain technology underlies these assets, enabling decentralized, secure, and relatively anonymous transactions. This technological innovation increases efficiency but also poses challenges to state authorities in maintaining financial stability, as demonstrated by differing regulatory responses in countries such as the United States, the European Union, and Singapore.

In many countries, crypto presents a regulatory dilemma. Its cross-border, anonymous, and difficult-to-trace nature makes it vulnerable to being used for crimes such as money laundering, online fraud, ransomware, and even terrorism financing (Europol, 2022). For example, Europol reports that crypto was involved in over €8 billion worth of illicit transactions in 2021. These crimes often span multiple jurisdictions, necessitating intensive international cooperation. The European Union has addressed this through the Markets in Crypto Assets (MiCA) Regulation, while other countries are still developing their frameworks.

Indonesia is not immune to these dynamics. Although crypto adoption continues to grow, national regulations remain fragmented. Bank Indonesia prohibits crypto as a means of payment, whereas Bappebti recognizes crypto as a legally traded commodity. This dual status has led to legal ambiguities, such as in the Manado District Court case No. 496/Pid.Sus/2022/PN Mnd, where Bitcoin obtained through skimming was ordered to be confiscated, yet the lack of technical regulations complicated implementation.

Conceptually, the legal status of crypto in Indonesia's criminal law is still underdeveloped. The Criminal Procedure Code (KUHAP) primarily addresses conventional evidence, so officials often interpret crypto assets as "intangible movable property." This interpretation has led to varying judicial practices and creates opportunities for pretrial challenges, highlighting the need for clearer norms. Without a comprehensive legal framework, confiscation of crypto assets risks undermining legal certainty, violating the rights of good-faith third parties, and eroding public trust in the justice system. Consequently, revising KUHAP or drafting specific legislation on digital assets is urgently needed.

At the international level, standards issued by the Financial Action Task Force (FATF) emphasize the implementation of Know Your Customer (KYC) and Anti-Money Laundering (AML) principles in crypto trading (FATF, 2021), the Budapest Convention on Cybercrime (2001) also highlights cross-border cooperation, yet Indonesia has not ratified it, relying instead on slower mutual legal assistance mechanisms (Europe, 2001). Political and legal considerations, including sovereignty concerns and alignment with domestic law, have been cited as reasons for this non-ratification.

Technical complexities further complicate enforcement. Crypto assets are intangible, difficult to trace without private keys, highly volatile, and cross-border. This requires specialized skills in digital forensics and blockchain analytics, which are

still limited in Indonesia (Fajarwati, 2022). The lack of technical regulations for seizure and confiscation can result in disputes over the rights of third parties acting in good faith.

Based on this context, the confiscation of crypto assets as evidence concerns not only technical enforcement but also legal certainty and harmonization of national regulations with international standards. Without comprehensive regulatory reforms and enhanced capacity of law enforcement officials, Indonesia will continue to face significant challenges in combating crypto-based cybercrime.

The objectives of this study include: To analyze the legal provisions for the confiscation of crypto assets as evidence in cybercrimes based on positive law in Indonesia and to formulate a more appropriate form of law enforcement regulations for the confiscation of crypto assets, taking into account the need for legal certainty and the dynamics of cybercrime.

The problem formulation in this research includes:

1. What are the legal provisions in force in Indonesia regarding the confiscation of evidence in the form of crypto assets in cybercrime cases?
2. What direction should the development of law enforcement regulations be applied to the confiscation of crypto asset evidence to be more effective and provide legal certainty?

2. METHODS

This article is a normative-empirical legal study, chosen to address the complex legal and practical issues surrounding the confiscation of crypto assets as evidence in cybercrime cases. This approach is suitable because it combines the examination of existing legal norms with empirical insights from stakeholders, allowing a more comprehensive understanding of both the regulatory framework and its practical implementation.

Normative legal research relies primarily on secondary legal materials, complemented by empirical inputs such as interviews to validate findings (Ibrahim, 2013). This method enables the researcher to analyze the direction of law enforcement regulations that should be applied to the confiscation of crypto assets as evidence to ensure greater effectiveness and legal certainty. Normative legal research also uses legal logic and reasoning from a normative perspective to interpret the law and discover its implications for practice.

This study applies the statute approach (statutory regulatory approach), which involves examining existing laws, regulations, and related legal instruments. This approach is relevant because the issue of crypto asset confiscation is directly governed by statutory provisions, and understanding these regulations is crucial to proposing practical law enforcement solutions.

The legal materials used in this study are sourced from primary, secondary, and tertiary sources. Primary sources include statutes, government regulations, and court decisions; secondary sources consist of academic journals, books, and reports;

and tertiary sources involve legal dictionaries and encyclopedias.

The research is descriptive and analytical, aiming to conceptualize the legal issues discussed and analyze relevant regulations to provide answers to the research questions. Analysis is conducted using a qualitative-descriptive method, focusing on interpretation, comparison, and critical evaluation of legal norms and practices.

3. RESULTS AND DISCUSSION

3.1. Legal Provisions Applicable in Indonesia Regarding the Confiscation of Evidence in the Form of Crypto Assets in Cybercrime Cases

In the legal system, the confiscation of evidence is an important instrument in enforcing criminal law, particularly to prevent perpetrators from enjoying the proceeds of their crimes. In general, provisions regarding confiscation and seizure are regulated in the Criminal Procedure Code (KUHAP). Article 39 of the KUHAP states that investigators have the authority to confiscate objects suspected of being obtained from criminal acts or used as a means of committing criminal acts. Furthermore, Article 46 paragraph (2) of the KUHAP emphasizes that confiscated objects can be determined to be confiscated for the state based on a court decision that has permanent legal force (Soesilo, 1996). This mechanism must be implemented in accordance with the legal principle of due process, ensuring that the rights of all parties, including the accused and third parties in good faith, are protected throughout the confiscation procedure

However, the Criminal Procedure Code (KUHAP), which was enacted in 1981, certainly did not envision the existence of digital evidence such as crypto assets. Therefore, regulations related to digital evidence are more clearly defined in sectoral regulations, for example Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was later amended by Law Number 1 of 2024. This law recognizes that electronic information and electronic documents can be used as valid evidence in court (Article 5 paragraph (1)). Thus, crypto asset transactions recorded in the blockchain system can be recognized as part of electronic evidence.

On the other hand, the legal status of crypto assets in Indonesia has undergone its own development. Bank Indonesia, through Bank Indonesia Regulation No. 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing, expressly prohibits the use of virtual currencies, including cryptocurrencies, as legal tender. However, through Bappebti Regulation Number 8 of 2021, crypto assets are recognized as tradable commodities on the Futures Exchange. This dualism causes the position of crypto in Indonesian law to be ambivalent: legal as an investment object, but illegal if used as a means of payment.

This normative conflict becomes even more apparent when linked to Law Number 7 of 2011 concerning Currency. Article 21 of the law affirms that the rupiah is the sole legal tender within the territory of the Unitary State of the Republic of Indonesia. Therefore, any transaction using crypto assets as a means of payment

can be classified as a violation of the law. This is emphasized in Bank Indonesia Regulation Number 19/12/PBI/2017, which prohibits financial technology providers from facilitating transactions using virtual currency.

However, as an investment instrument, crypto is legally treated under the framework issued by the Commodity Futures Trading Regulatory Agency (Bappebti). Through Bappebti Regulation Number 5 of 2019 concerning Technical Provisions for the Organization of Physical Crypto Asset Markets on Futures Exchanges, the government provides a basis for crypto to be traded as a futures commodity. This regulation is complemented by Bappebti Regulation Number 8 of 2021, which clarifies the guidelines for organizing physical crypto asset market trading. Under this legal regime, crypto assets are positioned not as currencies, but as digital commodities subject to exchange mechanisms. From a legal perspective, treating crypto as a commodity also implies recognition of property rights over digital assets, granting holders ownership and control over these assets under civil and commercial law principles.

The contradiction between the prohibition on the use of crypto as a means of payment and its recognition as a commodity has given rise to regulatory ambivalence. In legal literature, this situation is often referred to as legal dualism, where a single legal object has dual, contradictory statuses. This ambivalence not only creates legal uncertainty for the public but also opens up wide room for interpretation for law enforcement officials in enforcing regulations, particularly in criminal cases involving crypto (Fahira et al., 2024).

Furthermore, the existence of regulations scattered across various sectors demonstrates the country's partial approach to regulating crypto. The monetary sector, through Bank Indonesia, focuses on payment system stability, while the trade sector, through Bappebti, focuses on investment aspects (Peraturan Bappebti No. 8 Tahun 2021 Tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, 2021). This difference in focus creates potential jurisdictional conflicts, particularly regarding the oversight of cross-border crypto transactions, which could have implications for money laundering and terrorism financing (Asia Law Portal, 2023). Therefore, several academics emphasize the importance of integrated regulations that unite monetary, trade, and criminal law aspects within a single, comprehensive framework (Fahira et al., 2024).

Indonesia's situation differs from several other jurisdictions that have adopted a unified approach to crypto assets. The European Union, for example, through its 2023 Markets in Crypto-Assets Regulation (MiCA), comprehensively regulates the legal status, trading procedures, consumer protection, and oversight mechanisms for crypto assets (European Commission, 2023). Japan, through its Payment Services Act, also stipulates that crypto is a limited legal payment asset with a strict oversight regime (Financial Services Agency (Japan), 2020). This comparison demonstrates that Indonesia is still in the early stages of establishing a solid crypto legal framework and needs further development harmonization of regulations so as not to

create legal loopholes in criminal enforcement or investor protection (Otoritas Jasa Keuangan (OJK), 2023).

In judicial practice, this problem is increasingly evident. A case in point is Manado District Court Decision No. 496/Pid.Sus/2022/PN Mnd against defendant Ari Lufitasari, in which the Bitcoin proceeds of skimming were ordered to be confiscated by the state. Although the ruling affirmed the possibility of confiscating crypto assets, its implementation faced technical obstacles due to the lack of a clear legal mechanism for how the state could control, store, or convert these digital assets (Lihat Juga Widhartama, 2025). In addition, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (TPPU) Also relevant. Article 77 of the Money Laundering Law authorizes the courts to confiscate assets obtained through money laundering for the state. However, due to the intangible, borderless, and volatile nature of crypto assets, the implementation of this article remains controversial, particularly regarding ownership identification, value security, and international jurisdiction.

In law enforcement practice, storing crypto assets as evidence requires a technology-based secure custody mechanism. Crypto assets cannot be treated the same as conventional evidence because they rely on private keys, which are highly vulnerable to hacking and internal abuse. Therefore, the use of state digital wallets with cold storage and multi-signature systems is considered the most secure method. This was emphasized by Ryandi Yusuf, Sandiman Muda at Directorate V of the Intelligence Agency (JAM), who emphasized that minimum security standards must include the use of cold storage, multi-signature wallets, and high-level encryption to prevent the loss of digital evidence (Komunikasi pribadi, 12 Agustus 2025).

Beyond technical security aspects, crypto asset price volatility poses a serious challenge in the confiscation process. The highly fluctuating value of crypto assets can be detrimental to both the state and victims if not promptly managed. Therefore, regulations are needed to regulate the mechanism for converting confiscated crypto assets into rupiah at specific times. Ryandi Yusuf explained that such policies have been implemented in several countries, such as Japan and South Korea, which have measured liquidation procedures to maintain the stable value of evidence (Komunikasi pribadi, 12 Agustus 2025).

Another important issue is protecting the rights of third parties acting in good faith. In practice, criminally obtained crypto assets are often mixed with legitimate assets in a single digital wallet, potentially violating third-party ownership rights if there is no clear separation mechanism. Yudi Ariyanto Tri Santosa, Head of Intelligence at the Attorney General's Office Balikpapan, the State Attorney General, emphasized that the lack of detailed SOPs for the seizure of crypto assets could hamper legal legitimacy and even risk pretrial challenges. He emphasized the need for blockchain analytics-based tracing to ensure legitimate ownership and protect the constitutional rights of third parties (Komunikasi pribadi, 31 Juli 2025).

From an institutional perspective, obstacles arise from overlapping authority between the Police, the Prosecutor's Office, Bappebti, and the Financial Services Authority (OJK). Lukas Abraham Sembiring emphasized that the establishment of a special unit under the Prosecutor's Office would be an effective solution. This unit should be equipped with blockchain experts, digital auditors, and cybersecurity experts to ensure the professional management of digital evidence. This view is also supported by Ida Bagus Putu Widnyana, who stated that without specific regulations, law enforcement officials will continue to be trapped in extensive interpretations of the Criminal Procedure Code (KUHP) and the Money Laundering Law (UU TPPU), potentially leading to disparities in practice (Komunikasi Pribadi, 13 Agustus 2025).

Integration with international standards is an absolute necessity. The Financial Action Task Force (FATF), in its Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs (2021), emphasized the obligation of countries to have mechanisms for tracing, freezing, and confiscation of virtual assets. Lukas Abraham Sembiring stated that Indonesia must immediately adopt FATF standards to avoid difficulties in mutual legal assistance (MLA) cooperation and to ensure the national legal system has global legitimacy in addressing cross-border crimes involving crypto assets (Komunikasi Pribadi, 31 Juli 2025).

Based on the existing legal framework, it can be concluded that regulations regarding the confiscation of crypto assets in Indonesia are still fragmented and scattered across various regulations, including the Criminal Procedure Code (KUHP), the ITE Law, the Money Laundering Law, and the regulations of the Commodity Futures Trading Regulatory Agency (Bappebti). There is no single regulation that comprehensively governs the procedures for confiscating crypto assets as evidence in cybercrimes. This situation often leads law enforcement officials to rely on legal analogies and practices in case handling. As a result, legal certainty is weakened, even though it is crucial for supporting effective law enforcement in the digital age. A critical reflection suggests that Indonesia could benefit from adopting integrated regulatory frameworks similar to the European Union's MiCA Regulation, which combines oversight, market transparency, and consumer protection to address regulatory fragmentation in crypto asset governance.

3.2. Directions for the Development of Law Enforcement Regulations that Should Be Applied in the Confiscation of Crypto Asset Evidence to be More Effective and Provide Legal Certainty

The direction of developing law enforcement regulations for the confiscation of crypto asset evidence in Indonesia must be directed towards the formation of regulations that are comprehensive, explicit, and adaptive to developments in digital technology. Currently, the Criminal Procedure Code (KUHP) still focuses on conventional evidence, while digital assets such as crypto have not been explicitly

regulated. Article 39 paragraph (1) of the KUHAP does allow for the confiscation of objects or bills suspected of originating from criminal acts, but its application to crypto assets still raises questions. This issue remains open to multiple interpretations and creates uncertainty in enforcement. Therefore, a revision of the Criminal Procedure Code (KUHAP) or the creation of a specific law regarding digital assets is necessary to explicitly regulate the mechanisms for tracing, freezing, storage, and even execution of confiscation.

The development of regulations for the confiscation of crypto assets in Indonesia cannot be limited to the normative framework of the Criminal Procedure Code (KUHAP), which focuses on conventional evidence. In an interview, Ryandi Yusuf, the Young Detective of the Directorate V of Intelligence, emphasized that without clear national technical standards, law enforcement officers tend to interpret their own methods for securing digital evidence. He cited the example of investigators who might simply store private keys or seed phrases without using adequate security protocols, risking asset leakage. He argued that this demonstrates the need for comprehensive, technically sound regulations to mitigate the vulnerability of practices in the field (Komunikasi Pribadi, 12 Agustus 2025). This finding underscores the urgency of revising the KUHAP or establishing derivative technical regulations to ensure uniform standards and prevent inconsistent practices.

Similarly, Yudi Ariyanto Tri Santosa, Head of Intelligence at the Balikpapan District Attorney's Office, sees a broader issue of legal legitimacy. He believes that if the seizure and confiscation of crypto assets are carried out solely based on an expansive interpretation of Article 39 of the Criminal Procedure Code, such actions are vulnerable to pretrial challenges. For instance, a defendant could challenge the legality of confiscation under the principle of legality (*nullum crimen sine lege*), arguing that the KUHAP provides no explicit legal basis. He believes that without an explicit legal basis, law enforcement officers will always face the risk of lawsuits for alleged arbitrary actions. Therefore, revising the Criminal Procedure Code or establishing a specific law on digital assets is not only important but urgent to maintain legal legitimacy (Komunikasi Pribadi, 31 Juli 2025).

Ida Bagus Putu Widnyana also expressed a critical view. He believes that the practice of extensive interpretation of the Criminal Procedure Code (KUHAP) regarding crypto assets is merely a temporary solution that cannot be sustained in the long term. He believes that disparities in practice between regions are already beginning to emerge, with some authorities viewing crypto as legitimate evidence for confiscation, while others remain hesitant to do so. These disparities create uncertainty in law enforcement and can erode public trust in the justice system. In this context, he advocates for regulations specifically governing the tracing, freezing, and execution mechanisms for crypto assets, so that they do not depend on the individual interpretation of the authorities (Komunikasi Pribadi, 13 Agustus 2025).

Meanwhile, Lukas Abraham Sembiring underscored the importance of technical aspects in evidence management. He emphasized that crypto assets should

not be stored haphazardly but should be placed in a state-owned digital wallet with a cold storage system disconnected from the internet and utilizing multi-signature security systems to prevent any single party from accessing the assets alone. He believes this system will ensure that seized assets remain intact until the execution stage, while also reducing the potential for abuse of authority within law enforcement agencies (Komunikasi Pribadi, 31 Juli 2025).

Furthermore, interviewees also emphasized that without integrating national regulations with international standards, Indonesia will have difficulty enforcing cross-border confiscation of crypto assets. This challenge is evident from the experience of countries that cooperate under the Mutual Legal Assistance (MLA) framework, where mutual recognition of digital asset seizure and forfeiture mechanisms is a prerequisite. Thus, the direction of legal development is not limited to updating the Criminal Procedure Code (KUHAP) but also synchronizing it with international standards as recommended by the FATF (FATF, 2021).

From a technical perspective, existing regulations also need to include digital forensic standards and mechanisms for securing crypto evidence. The intangible, decentralized, and private-key nature of crypto assets necessitates the use of cold storage-based digital wallets with multi-signature systems for greater security. Furthermore, the volatility of crypto values necessitates procedures for conversion to fiat currency to prevent losses to the state and victims. International practice demonstrates this approach in Japan and South Korea, where governments manage cold wallets and employ controlled asset liquidation mechanisms under clear legal authority. Including legal references or policies from these countries would strengthen this analysis.

The direction of legal development must also address potential overlapping authority between institutions, given the overlapping roles of the Police, Prosecutor's Office, Financial Transaction Reports and Analysis Center (PPATK), CoFTRA (Commodity Futures Trading Regulatory Agency), Financial Services Authority (OJK), and the National Cyber and Cryptocurrency Exchange Agency (BSSN). Without a clear delineation of authority, the seizure of crypto assets will be hampered by institutional conflicts. Therefore, new norms must define the authority for the seizure, storage, and management of crypto assets, with a transparent external oversight system. This aligns with the principle of public accountability as stipulated in the Law on Judicial Power (Law No. 48 of 2009) and ensures institutional checks and balances.

Indonesia's delay in adopting international standards not only creates legal loopholes but also impacts the country's financial reputation. The FATF has blacklist and greylist mechanisms for countries deemed non-compliant with anti-money laundering and anti-terrorism financing standards. As of 2025, Indonesia remains under ongoing evaluation by the FATF in terms of compliance. Strengthening digital asset confiscation mechanisms will support the country's progress toward full compliance. If Indonesia does not immediately integrate a mechanism for

confiscating crypto assets in accordance with FATF standards, the risk of diminishing investor confidence and increasing international transaction costs is a real threat (FATF, 2021).

Implementation barriers in Indonesia lie in fragmented authority. Ryandi Yusuf emphasized in an interview that crypto assets are still viewed differently by Bank Indonesia, Bappebti, and the Financial Services Authority (OJK), resulting in often asynchronous coordination between institutions. This situation hampers efforts to formulate unified regulations. He believes the successful adoption of international standards depends on the existence of a single institution with a clear mandate to regulate the seizure and forfeiture of digital assets (Komunikasi Pribadi, 12 Agustus 2025). To overcome this, a National Coordinating Body for Digital Asset Governance could be established. This body would integrate functions from Bappebti, PPATK, and OJK, serving as the central authority responsible for regulation, supervision, and coordination in cases involving crypto assets. Such an institution could function similarly to South Korea's Financial Intelligence Unit (KoFIU), ensuring synchronization and preventing overlapping authority.

Besides coordination challenges, technical capacity issues also pose a challenge. Yudi Ariyanto Tri Santosa emphasized that many regional officials lack an adequate understanding of blockchain technology, making it often difficult to execute court-ordered seizure orders. He believes that before discussing harmonization with the FATF, the government must first ensure increased technical capacity of law enforcement in the field so that international standards do not remain on paper (Komunikasi Pribadi, 31 Juli 2025). Currently, some institutions such as PPATK and Bareskrim have begun conducting training programs on digital forensic investigation and blockchain tracing, yet participation remains limited to central-level officers. Expanding these initiatives into continuous national training programs, including collaboration with universities and international agencies such as UNODC, would strengthen the human resource foundation needed for consistent implementation.

Learning from the experiences of other countries, South Korea successfully integrated FATF standards by establishing a *Crypto Asset Tracking Center* involving law enforcement officials, financial authorities, and technology experts. This center not only serves as a data clearinghouse but also ensures that MLA (Mutual Legal Assistance) requests related to crypto assets are promptly fulfilled. A similar model can be replicated in Indonesia to make cross-border tracing and freezing processes more efficient and credible. According to FATF's 2023 Mutual Evaluation Report on South Korea, this integrated model significantly improved asset recovery success rates and reduced cross-border tracing time. Implementing a similar framework, supported by Presidential Regulation or derivative technical regulations, would provide Indonesia with a stronger institutional and legal foundation for international cooperation.

Integration with international standards must also be embedded within the victim protection framework. Ida Bagus Putu Widnyana emphasized that confiscation of crypto assets should not only be oriented towards filling state coffers but also guarantee victims' rights to restitution. In this context, the principle is reinforced by Law No. 13 of 2006 jo. Law No. 31 of 2014 concerning the Protection of Witnesses and Victims, which mandates restitution as a key element of justice restoration. He argued that regulations aligned with the FATF could actually strengthen victims' positions, as international standards emphasize asset recovery mechanisms that prioritize restitution of losses resulting from criminal acts (Komunikasi Pribadi, 13 Agustus 2025). Therefore, future regulations must explicitly include procedures for asset redistribution and victim compensation following confiscation to ensure restorative justice principles are upheld.

In addition, new regulations must protect the rights of well-intentioned third parties and guarantee restitution for victims. Criminally obtained crypto assets are often mixed with legitimate assets in a single digital wallet, so without separation guidelines, constitutional ownership rights can be violated. Article 28H paragraph (4) of the 1945 Constitution emphasizes that private property rights may not be taken arbitrarily, making regulations regarding objection mechanisms and ownership verification crucial. In this context, the use of blockchain forensics and chain analysis tools (such as Chainalysis or Elliptic) can be institutionalized to verify ownership and trace fund flows. These technologies enable differentiation between illicit and legitimate crypto holdings, ensuring fairness in asset confiscation. The principle of *restitutio in integrum* also requires that proceeds from asset confiscation be prioritized for restitution of victims' losses, not simply for state coffers (Muladi & Arief, 2010).

Finally, the direction of legal development in Indonesia must be integrated with international standards. In its latest guidelines, the Financial Action Task Force (FATF) emphasizes the obligation of states to provide mechanisms for the seizure, freezing, and confiscation of virtual assets (FATF, 2020). In addition, the Budapest Convention on Cybercrime (Council of Europe, 2001) provides a framework for cross-border cooperation to address digital asset-based cybercrime. Adopting these international standards will strengthen the effectiveness of national law enforcement and enhance Indonesia's global legitimacy in addressing cross-border crimes involving crypto assets. In this regard, integration with international frameworks also aligns with Indonesia's Long-Term National Development Plan (RPJPN 2025–2045) and the National Human Rights Action Plan (RANHAM), which emphasize digital governance, rule of law, and protection of citizens' property rights in the digital era. Thus, the adoption of FATF and Budapest standards should be seen as a strategic step toward realizing these national objectives.

The lack of legal frameworks governing the confiscation of crypto assets often requires law enforcement officials to rely on extensive interpretations of the provisions of the Criminal Procedure Code (KUHAP) and the Anti-Money Laundering

Law, which leads to practical and doctrinal inconsistencies. This has led to disparities in practice across regions, with some investigators and prosecutors daring to confiscate crypto on the basis of "intangible movable property," while others refuse, citing the lack of explicit provisions. This situation clearly creates legal uncertainty for both the public and the authorities.

The absence of specific regulations also impacts the evidentiary aspect in court. Yudi Ariyanto Tri Santosa emphasized that judges ultimately require an explicit legal basis to authorize the seizure of crypto assets. According to him, if regulations are not established promptly, there is a risk of judges rejecting digital evidence or declaring the seizure invalid due to a violation of the principle of legality (*nullum crimen, nulla poena sine lege*). As Utrecht (1958) and Moeljatno (2008) have noted, this principle ensures that no act can be punished without a prior legal provision. Thus, the lack of norms not only impacts the investigation stage but can also undermine law enforcement efforts in court.

In addition to the issue of proof, the lack of norms also poses the risk of violating third-party rights. Ida Bagus Putu Widnyana warned that without detailed regulations regarding asset tracing and segregation mechanisms, the state could confiscate crypto assets belonging to well-intentioned parties. To mitigate this, regulations should mandate a pre-confiscation verification stage involving forensic tracing, ownership certification, and objection procedures accessible through digital platforms. Within the framework of a state governed by the rule of law, this situation is dangerous because it potentially violates citizens' constitutional rights, as stipulated in Article 28H paragraph (4) of the 1945 Constitution concerning the protection of private property rights.

From an institutional perspective, the lack of norms exacerbates overlapping authority between agencies. Ryandi Yusuf stated that as long as there are no regulations clearly defining the primary agency responsible for managing crypto assets derived from criminal activity, coordination between the Police, the Prosecutor's Office, Bappebti (Trading Commodity Futures Trading Regulatory Agency), and the Financial Services Authority (OJK) will continue to be asynchronous. This has the potential to lead to recurring conflicts of authority, with each agency claiming its own authority over handling crypto evidence. Hence, the establishment of a unified regulatory authority, or at least a cross-institutional coordination protocol under a Presidential Decree, is essential to ensure coherence and avoid jurisdictional disputes.

Ultimately, this normative vacuum also weakens Indonesia's position in international cooperation. Lukas Abraham Sembiring emphasized that other countries will only be willing to fulfill requests for legal assistance if Indonesia has a legal framework that meets global standards. In other words, the existence of comprehensive regulations that address the normative vacuum is not merely a domestic necessity but also key to Indonesia's legitimacy and credibility in the international legal system.

Thus, the direction of development of crypto asset confiscation regulations must emphasize four main pillars: (1) establishing comprehensive regulations, (2) strengthening technical standards and digital forensics, (3) affirming institutional authority and oversight mechanisms, and (4) integrating with international standards. These four pillars will ensure that crypto asset confiscation is not only legally valid, but also effective, transparent, and provides legal certainty in accordance with the principles of the rule of law in Indonesia. Reflecting on Indonesia's 2045 Vision, these pillars align with the broader national objective of building a just, technologically adaptive, and globally credible legal system. Therefore, the development of crypto confiscation regulations represents not merely a technical necessity, but a strategic direction in realizing Indonesia's digital legal transformation.

4. CONCLUSION

Indonesian legal provisions regarding the confiscation of evidence in the form of crypto assets in cybercrimes are still partial and scattered across various regulations. The Criminal Procedure Code (KUHAP) does not explicitly regulate the existence of digital assets, so law enforcement often relies on extensive interpretations, creating legal uncertainty and disparities in practice. Regulatory ambivalence is increasingly apparent with the prohibition on the use of crypto as a means of payment on the one hand, and its recognition as a futures commodity on the other hand, which gives rise to legal problems in judicial practice.

The development of law enforcement regulations for the confiscation of crypto assets needs to be directed towards the creation of comprehensive regulations aligned with international standards. These regulations must explicitly regulate the mechanisms for tracing, freezing, storage, and execution of confiscation, while clarifying the authority of different institutions to avoid overlapping jurisdictions. Furthermore, increasing the technical capacity of law enforcement officials in digital forensics and blockchain analytics is essential to ensure effective, legal, and legal certainty for the public.

5. SUGGESTION

The government needs to immediately formulate specific regulations that comprehensively govern the confiscation of crypto assets as evidence in cybercrimes. These regulations must cover procedures for confiscation, storage, management, and execution, while also protecting the rights of good-faith third parties and ensuring the restoration of victims' rights. Revision of the Criminal Procedure Code (KUHAP) or the creation of a specific law on digital assets is an urgent step to ensure legal certainty and maintain the legitimacy of criminal justice.

Furthermore, it is necessary to improve the technical capacity of law enforcement officers through digital forensics training, the use of blockchain analytics, and the provision of secure storage facilities such as cold storage and multi-signature wallets. The government also needs to emphasize the division of

authority between law enforcement agencies to avoid overlapping, and integrate national regulations with international standards, such as FATF recommendations and the Budapest Convention, to strengthen the effectiveness of cross-border cooperation in handling crypto-asset-based cybercrime.

REFERENCES

- Asia Law Portal. (2023). *Changing of the Guards in Indonesia's Crypto Asset Sector*. <https://www.asialaw.com/>
- Badan Pengawas Perdagangan Berjangka Komoditi. (2019). Peraturan Bappebti Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka. Jakarta: Kementerian Perdagangan RI.
- Badan Pengawas Perdagangan Berjangka Komoditi. (2021). Peraturan Bappebti Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto di Bursa Berjangka. Jakarta: Kementerian Perdagangan RI.
- Bank Indonesia. (2016). Peraturan Bank Indonesia Nomor 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran. Jakarta: Bank Indonesia.
- Bank Indonesia. (2017). Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial. Jakarta: Bank Indonesia.
- Chaum, D. (1983). Blind Signatures for Untraceable Payments, *Advances in Cryptology. Proceedings of the Springer-Verlag Crypto'82*, 3, 199–203.
- Europe, C. of. (2001). *Convention on Cybercrime. Budapest, 23.XI.2001*.
- European Commission. (2023). *Markets in Crypto-Assets (MiCA)*. https://finance.ec.europa.eu/digital-finance/crypto-assets_en?utm
- Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*. Europol.
- Fahira, S. H., Daimah, D., & Mu'amar, R. (2024). Cryptocurrency Regulation in Indonesia: Regulation Review and Potential Risks from A Cyber Law Perspective. *Indonesian Cyber Law Review*, 1(2). <https://doi.org/https://doi.org/10.59261/iclr.v1i2.3>
- Fajarwati, E. (2022). Blockchain Forensics dan Tantangan Penegakan Hukum di Era Kripto. *Jurnal Hukum Dan Teknologi*, 12(2).
- FATF. (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*. <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html>
- FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service*. FATF. <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA->

VA-VASP.html

Financial Services Agency (Japan). (2020). *Payment Services Act (as amended)*.
<https://www.japaneselawtranslation.go.jp/en/laws/view/3965/en>

Ibrahim, J. (2013). *Teori & Metodologi Penelitian Hukum Normatif*. Bayu Media.

Muladi, & Arief, B. N. (2010). *Teori-Teori dan Kebijakan Pidana (Cet.4)*. Alumni.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
<https://bitcoin.org/bitcoin.pdf>

Otoritas Jasa Keuangan (OJK). (2023). *Press Release: OJK Commits to Strengthen Supervision of Financing and Technology Innovation Financing in the Financial Sector*.
[https://www.ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Documents/Pages/OJK-Commits-To-Strengthen-Supervision-of-Financing-and-Technology-Innovation-Financing-In-The-Financial-Sector/PR - OJK COMMITS TO STRENGTHEN SUPERVISION OF FINANCING AND TECHNOLOGY INNOVATION FINANCING IN THE FINANCIAL SECTOR.pdf](https://www.ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Documents/Pages/OJK-Commits-To-Strengthen-Supervision-of-Financing-and-Technology-Innovation-Financing-In-The-Financial-Sector/PR-OJK-COMMITS-TO-STRENGTHEN-SUPERVISION-OF-FINANCING-AND-TECHNOLOGY-INNOVATION-FINANCING-IN-THE-FINANCIAL-SECTOR.pdf)

Peraturan Bappebti No. 8 Tahun 2021 Tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka (2021).
<https://bappebti.go.id/>

Republik Indonesia. (1981). Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHP). Lembaran Negara RI Tahun 1981 No. 76.

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 No. 58.

Republik Indonesia. (2010). Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Lembaran Negara RI Tahun 2010 No. 122.

Republik Indonesia. (2011). Undang-Undang Nomor 7 Tahun 2011 tentang Mata Uang. Lembaran Negara RI Tahun 2011 No. 64.

Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2024.

Pengadilan Negeri Manado. (2022). Putusan Nomor 496/Pid.Sus/2022/PN Mnd (perkara Ari Lufitasari, Skimming ATM).

Yusuf, R. (2025, Agustus 12). Wawancara pribadi dengan Sandiman Muda Direktorat V JAM Intelijen.

Santosa, Y. A. T. (2025, Juli 31). Wawancara pribadi dengan Kasi Intel Kejaksaan Negeri Balikpapan.

Widnyana, I. B. P. (2025, Agustus 13). Wawancara pribadi dengan Kepala Seksi Tindak Pidana Umum Kejaksaan Negeri Surabaya.

Sembiring, L. A. (2025, Juli 31). Wawancara pribadi dengan Kasi Wilayah III Pra-Penuntutan Direktorat D.

Soesilo, R. (1996). *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*. Politeia.

Widhartama, I. G. (2025). *Kepastian Hukum Terhadap Perampasan Barang Bukti Aset Kripto dalam Tindak Pidana Siber*. Universitas Sam Ratulangi.