TRANSPUBLIKA
Precise. Resilience. Felicitous.

Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v4i2.1679

Original Article

Establishing the Legal Basis for Crypto Asset Confiscation: A Critical Study on the Challenges of Cybercrime Law Enforcement in Indonesia

Muhamad Rizqi Yudha Pratama[1*], Chairul Muriman[2], Surya Nita[3]

[1-3]Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Depok, Indonesia
Email: [1)] yudhapratamarz@gmail.com, [2)] cak_iir1966@yahoo.com, [3)] suryanita.sksgui@gmail.com

Received : 13 March - 2025
Accepted : 12 May - 2025
Published online : 14 May - 2025

Abstract

Cryptocurrency offers high potential profits but also poses significant challenges for law enforcement, especially in the context of cybercrime. Cybercrime encompasses various illegal activities conducted through computer networks and the internet, such as online fraud, data theft, and money laundering. The purpose of this research is to analyze the current legal provisions in Indonesia governing the seizure of cryptocurrency in cybercrime cases and to examine legal solutions that can be implemented to address the regulatory gaps related to the seizure of cryptocurrency in cybercrime cases in Indonesia. This research employs a qualitative research method, using law enforcement theory as the analytical framework. The results indicate that the seizure of cryptocurrency in cybercrime cases in Indonesia is still relatively new and faces various challenges, including regulatory ambiguity and a lack of understanding among law enforcement regarding blockchain technology. Although cryptocurrencies are recognized as tradable digital commodities, existing legal provisions, such as those in the Indonesian Criminal Procedure Code (KUHAP) and the Attorney General's Regulation No. 7 of 2023, remain limited and require coordination with the Commodity Futures Trading Supervisory Agency (Bappebti) and physical traders. The absence of specific regulations regarding the procedure for seizing cryptocurrency calls for a comprehensive legal approach, including the formulation of clear regulations, strengthening the existing legal framework, and enhancing law enforcement capacity. With these measures, it is hoped that law enforcement against cybercrime can be conducted more effectively, providing legal certainty and protecting the public from the risks of cybercrime.

Keywords: Blockchain Regulation, Cybercrime Law Enforcement, Crypto Asset Confiscation, Cryptocurrency Seizure, Digital Forensics.

1. Introduction

The development of information and communication technology has had a significant impact on various aspects of life, including the economy and finance. One of the innovations that has emerged alongside technological advancements is crypto assets, which include digital currencies such as Bitcoin, Ethereum, and various other tokens. Crypto assets offer the potential for high profits but also pose significant challenges in terms of law enforcement, particularly regarding cybercrime.

Cybercrime encompasses various illegal activities conducted through computer networks and the internet, such as online fraud, data theft, and money laundering. The existence of crypto assets provides new opportunities for criminals to engage in illegal activities using the anonymity offered by blockchain technology. This phenomenon necessitates that countries, including Indonesia, promptly establish an adequate legal

framework regarding the confiscation of crypto assets to enable effective and efficient law enforcement (Reedy, 2024).

To date, regulations concerning crypto assets in Indonesia remain unclear and fragmented. Existing regulations issued by the Commodity Futures Trading Regulatory Agency (BAPPEBTI) and Bank Indonesia focus more on the trading aspects and use of crypto assets as investment instruments. However, this legal uncertainty presents a unique challenge for law enforcement in handling cybercrime cases involving crypto assets. Confiscating assets obtained from crimes an important step in law enforcement which is often hindered by deficiencies in the existing legal framework.

This research is motivated by the issue of legal vacuums that lack the legal authority needed by all law enforcement officers, including investigators from the Indonesian National Police (Polri), in confiscating crypto assets during investigations. This legal vacuum creates challenges in executing confiscation processes effectively and in accordance with applicable legal principles. Without clear and comprehensive legal regulations, Polri investigators face difficulties in determining the steps to take regarding crypto asset confiscation, such as security procedures, storage, and the use of digital evidence. This can impact the integrity of investigations, operational efficiency, and accountability of investigators. Therefore, this study aims to identify issues related to the legal vacuum used as a basis for confiscating crypto assets such as security procedures, storage, and the use of digital evidence and analyze its implications for investigative processes while formulating police regulation policies (Perpol) to serve as a legal basis for confiscating crypto assets according to the needs and standards of law enforcement in Indonesia.

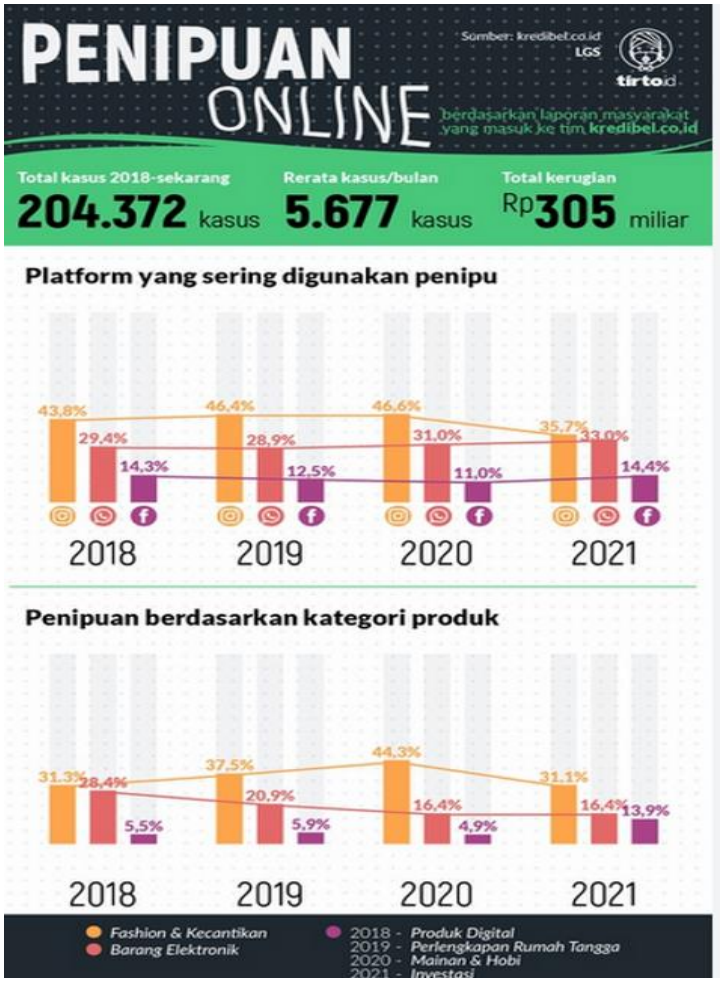
The need for a legal basis for confiscating crypto assets arises alongside digital technology developments that have changed societal behavior from initially storing assets in physical forms like gold and property to increasingly favoring digital asset storage, including crypto assets. This shift creates an urgent need for adequate legal regulations in the process of confiscating crypto assets, considering that these assets have characteristics distinct from conventional physical assets. Crypto assets can be stored in digital wallets requiring special handling during confiscation processes, such as access to private keys and management of complex digital security. Additionally, instant cross-border transactions via blockchain networks also present unique challenges regarding evidence collection and tracing the origins of crypto assets involved in illegal activities (Rosales et al., 2023).

The prevalence of transnational cybercrime further underscores the necessity for a solid legal foundation for executing crypto asset confiscations to be established and reinforced promptly. Transnational cybercrime exploits the ease and anonymity offered by crypto assets to facilitate their illegal activities. This complicates investigation and confiscation processes because challenges arise in gathering evidence, tracking transactions crossing national borders, and identifying cybercriminals who often use privacy-protecting technologies and tools.

Several examples of cybercrime cases in Indonesia involving crypto assets include investment fraud perpetrated by international networks. One notable case involves money laundering from fraud through a Binary Option Platform application called Binomo committed by suspects Indra Kenz and Nathania Kesuma. They stored crypto assets worth IDR 35 billion at Indodax Exchange. Another example is a fraudulent investment project through a fake Initial Coin Offering (ICO) named Giza, where scammers deceived approximately 1,000 individuals with losses exceeding USD 2 million or equivalent to IDR 22 billion. Additional cases involve fraudulent investments such as those executed by Doni Salmanan through binary option investment scams via Quotex, which resulted in losses

amounting to IDR 24 billion; Reza Paten's fraud through Net89 trading robots causing losses of IDR 2 trillion; and Dinar Wahyu Septian alias Wahyu Kenzo's investment scam with Auto Trade Gold robots leading to losses totaling IDR 9 trillion. Another instance involves scams conducted via email or fake websites mimicking cryptocurrency exchange platforms or digital wallets where perpetrators employ phishing techniques to steal users' personal information or send malware that can compromise access to users' crypto wallets (Lintasarta, 2023).

Based on these examples of cases above, it is evident that in Indonesia, cybercrime involving fraud utilizing social engineering techniques where perpetrators exploit victims' psychology and personal information to gain access to their crypto wallets or critical financial information which is currently trending and has victimized many individuals. This can be observed from the following report data:



Source: Hidayat (2021)

Figure 1. Trends in Online Fraud based on the Platforms and Product Categories (2018-2021)

Based on the figure 1 above, the highest cybercrime cases in Indonesia over the past seven years have been online fraud with 12,611 reports, followed by defamation and slander with 5,281 and 5,124 reports, respectively, and extortion with 2,628 reports. WhatsApp is the platform most frequently reported by the public with 15,297 complaints, followed by Instagram (6,875 reports), phone/SMS (4,678), and Facebook (3,936 reports). However, Muhammad Yunnus Saputra (CCIC Chief Analyst) explains that online fraud most often occurs on Instagram, where perpetrators use the platform to lure victims and then conduct

transactions via WhatsApp. The problem lies in Instagram's data storage being located overseas, making law enforcement difficult due to privacy regulations. Data from kredibel.co.id also shows an increase in fraud through Instagram, reaching 46.59% in 2020, with WhatsApp and Facebook following in subsequent positions.

This issue highlights the vulnerability of Indonesian society to online fraud attacks over the past few years. The impacts of this vulnerability span various aspects, including social, economic, security, and public peace. Socially, the rise in online fraud cases has decreased public trust in digital transactions, social media, and online communication, potentially hindering interactions and collaborations on digital platforms. Economically, the financial losses caused by online fraud are significant for both individual victims and businesses involved in addressing these cases, such as banking services and e-commerce platforms. From a security perspective, law enforcement's inability to effectively handle these cases due to limited access to data stored abroad and regulatory challenges regarding platform privacy increases the risk of broader cybercrimes. These crimes could escalate into more serious threats like money laundering or funding illegal activities. Finally, the impact on public peace is evident as many victims experience anxiety and uncertainty when using digital technology, leading to psychological distress and a greater sense of insecurity in daily life. This underscores the need for more serious efforts to develop regulations responsive to technological advancements and to strengthen public digital literacy. The issue also highlights the necessity of raising awareness and cybersecurity education among Indonesian society and businesses (Kabra & Gori, 2023).

Indonesia has already engaged in international cooperation to address cybercrime issues. For instance, it collaborates with ASEAN countries through the establishment of the ASEAN Regional Computer Emergency Response Team (ASEAN-CERT), a virtual cybersecurity team comprising analysts and incident responders from all member states (Caianiello & Camon, 2021). ASEAN-CERT plays a key role in enhancing ASEAN's regional cybersecurity resilience amidst an increasingly complex cyber threat landscape. Additionally, Indonesia has partnered with the United Kingdom through forums such as the United Nations Group of Governmental Experts (UN GGE). This forum reinforces their commitment to strengthening cybersecurity cooperation and reaching mutual understandings on cyber issues while voicing concerns over escalating cyberattacks and their detrimental impacts (Blandin et al., 2020). Through such collaborations, Indonesia aims to collect evidence, pursue perpetrators, and recover stolen assets through crypto assets resulting from cybercrimes.

However, Indonesia continues to face challenges in maintaining and developing information technology infrastructure. The country struggles with improving IT infrastructure, developing qualified human resources in this field, and adopting the latest cybersecurity practices. This has left Indonesia lagging behind on the global IT innovation map, affecting its competitiveness on an international scale (Syamsu et al., 2022). Another challenge faced by Polri (the Indonesian National Police) as one of the government institutions tasked with enforcing laws against cybercrime is the lack of solid legal regulations serving as a legal basis for all law enforcement officers particularly Polri investigators for confiscating crypto assets derived from money laundering crimes linked to fraud as their predicate offenses. This issue significantly impacts the effectiveness and efficiency of investigations and law enforcement concerning crypto assets involved in crimes. Without clear and comprehensive legal regulations with binding authority, Polri investigators face difficulties determining steps for confiscating crypto assets such as security procedures, storage methods, or handling digital evidence which can affect investigation integrity, operational efficiency, and investigator accountability (Suhartanto, 2024).

The challenges of confiscating crypto assets can be observed in cases like that of Alven Desnecmen a victim of electronic fraud using a "Pig Butchering" scheme that simulated trading via https://metavex.asia resulting in losses amounting to IDR 690 million. This case is documented under LP/A/14/XI/2023/SPKT.DITTIPIDEKSUS/BARESKRIM dated November 3rd, 2023. It represents a form of money laundering crime as regulated under Articles 3 and/or 4 and/or 5 Jo Article 10 of Law No. 8 of 2010 on Money Laundering Prevention and Eradication (PPTPPU) alongside Article 378 Jo Article 55 Paragraph (1) Point-1 Jo Article 56 of Indonesia's Criminal Code (KUHP). The suspects include Mei Ring alias Angel; Leliyana; and Choong Yeng Seng alias Hugo alias Freeman.

In Alven Desnecmen's case review process during investigations by Polri investigators uncovered evidence involving communication devices containing Binance a major international crypto exchange application where suspects admitted holding crypto assets obtained from fraudulent activities stored within Binance. Consequently, Polri investigators needed to confiscate these crypto assets as evidence for money laundering crimes linked directly back toward fraudulent acts committed against Alven Desnecmen.

However, 'Binance' does not operate within Indonesian jurisdiction, necessitating international coordination efforts by Polri investigators during asset seizure processes involving Binance-held accounts/assets stored externally outside Indonesia's territorial reach. This requires intermediary exchanges such as Tokocrypto (now acquired under Binance umbrella operations), facilitating indirect coordination pathways enabling investigative inquiries and extending seizure requests onto Binance-linked accounts/assets. These accounts become indirectly accessible via Tokocrypto intermediary channels, bridging jurisdictional gaps that would otherwise hinder direct procedural accessibilities. This addresses the lack of domestic jurisdictional reach over Binance operations externally domiciled beyond Indonesian sovereign borders, which currently lack enforceable regulatory frameworks governing cross-border seizure procedures and crypto-assets evidentiary admissibility frameworks.

This research aims to analyze the challenges faced in enforcing cybercrime laws related to crypto assets in Indonesia and to formulate recommendations for establishing a strong legal basis for crypto asset seizure. This study is expected to contribute to the development of legal policies that are adaptive and responsive to the dynamics of technological advancements and cybercrime.

Based on the background above, this research aims to:

1) Explain the current legal provisions in Indonesia that regulate the seizure of crypto assets in cybercrime cases.
2) Describe the legal solutions that can be implemented to address the regulatory gap related to the seizure of crypto assets in cybercrime cases in Indonesia.

2. Literature Review

2.1. Law Enforcement Theory

According to John Austin, a British philosopher cited by Soerjono Soekanto (2007), law is a command issued by the highest authority or sovereign power. Austin argues that law consists of instructions given by an individual who possesses both reason and power, with the purpose of regulating the behavior of others. In Austin's view, legitimate law is that which is enacted by the ruler for its subjects and comprises four main elements: command, sanction, obligation, and sovereignty.

Meanwhile, Friedrich Karl von Savigny, a German legal historian cited by Soerjono Soekanto (2007), views law as a reflection of the legal consciousness within a society (*Volksgeist*). According to him, all laws originate from customs and societal beliefs rather than from lawmakers.

Satjipto Rahardjo (2008) states his perspective on law enforcement, emphasizing that it is the concrete implementation of law in people's daily lives. Once a law is established, its enforcement in society becomes the essence of law enforcement. Although it is sometimes referred to as law application or law enforcement, the core idea remains the actualization of law in practice.

Based on various explanations of law enforcement, it can be understood that the primary objective of lawmaking is to ensure its effectiveness in achieving legal goals. Substantially, the purpose of legal norms is to create balance and harmony in interactions between individuals. People tend to comply with the law due to the fear of negative consequences for violations. This leads to the perspective that laws with strict sanctions are effective in maintaining social order.

However, the effectiveness of law and the role of sanctions in maintaining social order involve juridical, sociological, and philosophical aspects. Theories ranging from Hans Kelsen's legal positivism to sociological perspectives on recognition and authority highlight different dimensions of law. Herbert L. Packer (as cited in Soerjono Soekanto, 2007) emphasizes the importance of criminal sanctions in maintaining public welfare and addressing threats while ensuring a balance with individual freedoms. Other relevant factors include well-designed legislation, proportional sanctions, and public participation in law enforcement. Principles of democracy, moral values, and rational criminal law policies are also key to maintaining legal effectiveness, which significantly depends on public perception and participation in legal compliance.

According to Soerjono Soekanto (2007), several factors influence law enforcement. These factors are explained in detail below:

1) Legal Factors
   The concept of law involves regulations, rules, and norms that serve as a standard for society's interactions, ensuring order and stability. This is primarily limited to laws, which are defined as general written regulations enacted by the central or regional government. Laws in a material sense include national regulations that apply to all citizens or specific groups, as well as local regulations that are only applicable in a particular area. Weaknesses and deficiencies in legal formulations or norms can lead to failures in law enforcement. Sometimes, legal provisions or norms are unclear, allowing for multiple interpretations and causing uncertainty.
2) Law Enforcement Factors
   Every law enforcement officer holds a position and role within society. Their social status determines their place within the societal structure. This status includes rights and obligations, which encompass the duties and responsibilities of each law enforcement officer in carrying out their tasks.
3) Infrastructure of Facilities Factors
   Infrastructure and facilities, including well-educated and skilled personnel, a well-organized system, adequate equipment, sufficient financial resources, and more, are essential for effective law enforcement. Without these necessary resources, law enforcement cannot be carried out efficiently.

4) Societal Factors
Law enforcement originates from society and aims to achieve peace within the community. Society plays a significant role in influencing and determining the success of law enforcement. Social harmony depends on legal awareness and adherence to applicable regulations. Legal awareness includes the values that society holds regarding existing or expected laws. Cultural values within a society should also be considered in law enforcement (Hafizhah et al., 2023).

The four factors influencing law enforcement—legal factors, law enforcement officers, infrastructure or facilities, and societal factors form a crucial foundation for maintaining order and justice in a community. Additionally, these factors complement and interact with each other to uphold the integrity of a country's legal system. They cannot be separated and serve as key benchmarks in assessing the effectiveness and quality of a legal system's enforcement.

3. Methods

This study employs a qualitative research approach to enable the researcher to describe and communicate the findings, particularly regarding crypto assets, the comparison between crypto asset seizure practices in Indonesia and other countries, as well as their implications and the policy formulation of police regulations (Perpol) on crypto asset seizure by investigators at Bareskrim Polri.

Additionally, this research adopts an exploratory descriptive research type. Descriptive research aims to provide a comprehensive overview or description of the phenomenon being studied. In this study, the research seeks to explain the legal vacuum issue, specifically regarding police regulations (Perpol) on crypto assets. The objective is to offer a clear and comprehensive depiction of the policy formulation of police regulations (Perpol) on crypto assets to ensure their optimal use in law enforcement (Kristiani, et al., 2022).

Exploratory research is a type of study conducted when knowledge about a phenomenon is still limited or not yet well understood. This research aims to explore, describe, and understand the phenomenon in greater depth. In this study, the use of an exploratory descriptive approach is intended to delve deeper into the impact of the legal vacuum, particularly concerning police regulations (Perpol) on crypto assets. Through an exploratory approach, this study can identify previously undiscovered issues, gain new insights, and contribute to a more comprehensive understanding of the policy formulation of these police regulations (Perpol).

4. Results and Discussion

This study focuses on the analysis of the legal provisions in force in Indonesia regarding the confiscation of crypto assets in cybercrime cases, as well as efforts to formulate legal solutions to overcome the existing regulatory gaps. The limitations of the problem include: (1) identification and evaluation of current legal regulations, such as the Criminal Procedure Code (KUHAP), Attorney General's guidelines Number 7 of 2023, and the regulations of the Commodity Futures Trading Supervisory Agency (Bappebti), which regulate the procedures for confiscating crypto assets; (2) analysis of law enforcement challenges, including regulatory ambiguity, lack of understanding of blockchain technology by law enforcement officers, and the complexity of confiscating digital and transnational crypto assets; and (3) formulation of policy recommendations in the form of comprehensive police regulations (Perpol) to regulate

procedures for securing, storing, and using digital evidence of crypto assets, in order to ensure the effectiveness, legality, and accountability of the confiscation process in enforcing cybercrime law in Indonesia. This study does not discuss the technical aspects of managing crypto assets outside the context of confiscation or types of cybercrime that do not involve crypto assets. The implication is that this research will produce policies that increase the effectiveness, legality, and accountability of the confiscation of crypto assets by the Police, reduce the risk of investigative errors, and ensure legal certainty, without discussing the technical aspects of crypto management outside of confiscation or cybercrimes that do not involve crypto assets.

4.1. Current Legal Provisions in Indonesia Regulating the Seizure of Crypto Assets in Cybercrime Cases

Cryptocurrency is one form of digital asset, alongside Non-Fungible Tokens (NFTs), tokenized assets, and other types of digital assets. These assets function as a medium of exchange that uses cryptography to secure financial transactions, control the creation of new units, and verify asset transfers. The characteristics of cryptocurrencies are pseudo-anonymous, where transactions can be viewed and recorded publicly through blockchain technology, but user identities remain undisclosed. Cryptocurrencies can be used as payment tools and investment instruments, with some countries, such as El Salvador and the Central African Republic, legalizing their use as payment methods, while others prohibit them. Despite being banned as a payment tool in some places, cryptocurrencies are recognized as high-potential investment instruments.

Blockchain technology plays a crucial role in cryptocurrencies by offering decentralization, transparency, and permanence in financial transactions without intermediaries. Blockchain operates by distributing a digital ledger that accurately and quickly records every transaction while allowing verification by various parties. The uniqueness of blockchain fosters trust in recorded data, minimizes errors and crimes such as hacking, and reduces costs by eliminating traditional intermediaries like banks and advocates. Cryptocurrency transactions require crypto wallets to send and receive assets, enabling users to transact anytime and anywhere (U.S. Department of Treasury, 2022).

In Indonesia, cryptocurrencies are regulated as digital commodities that can be traded on the Futures Exchange, overseen by the Commodity Futures Trading Regulatory Agency (Bappebti). Physical Crypto Asset Traders approved by Bappebti conduct cryptocurrency transactions using Rupiah currency. Users must transfer funds to designated accounts for cryptocurrency transactions and comply with the travel rule principle to prevent illegal activities. Although cryptocurrency storage is regulated, there is currently no official entity acting as a Crypto Asset Storage Manager. Cryptocurrencies are considered intangible movable property under the definition in Indonesian civil law.

The seizure of cryptocurrencies in Indonesia as evidence in criminal cases is still relatively new and less common, even though the development of these assets began in 2010. Cryptocurrencies started gaining recognition among Indonesians around 2016, but challenges such as the need for advanced technology, low understanding of how they work and their utility, as well as fluctuating values hinder public interest in investing. Additionally, cryptocurrencies are often used by criminals to conceal proceeds from crimes because crypto transactions do not require intermediaries and information is stored in code form on blockchain that is difficult to alter. The confidentiality inherent in crypto transactions also makes them an attractive medium for money laundering (Yanwardhana, 2024).

From a legal perspective, Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes (TPPU Law) covers various types of crimes that may involve

money laundering proceeds. The Financial Transaction Reports and Analysis Center (PPATK) states that the main challenge in tracing cryptocurrencies lies in user confidentiality and protection provided by blockchain technology. To address this issue, PPATK analyzes each transaction and attempts to link involved parties.

Although tracing cryptocurrencies in criminal cases appears challenging, there are examples of seizures that have occurred in Indonesia, such as in the case of PT Asabri suffering significant losses due to corruption where suspects used Bitcoin to hide corruption proceeds. Another example is the case of Indra Kenz involving false news dissemination and money laundering through cryptocurrency transactions. Currently, positive law in Indonesia does not yet detail procedures for seizing cryptocurrencies; thus, seizures follow provisions under the Criminal Procedure Code (KUHAP).

The procedure for seizing cryptocurrencies involves several steps, including coordination with various parties such as Bappebti and physical crypto asset traders. Investigators must request information and documents related to suspected cryptocurrency transactions, including the perpetrator's crypto wallet. Subsequently, investigators may seek permission from the court chairman to perform seizures; in urgent situations, investigators may seize assets directly and report these actions to the court for approval. Attorney General's Guidelines Number 7 of 2023 has been issued to handle cryptocurrencies as evidence in criminal cases due to their increasing role in meeting society's needs for efficient transactions free from government or financial institution intervention. Cryptocurrencies defined as intangible digital commodities have been recognized as tradable commodities in Indonesia under applicable regulations. However, the anonymous nature of cryptocurrency transactions makes them vulnerable to misuse for concealing crime proceeds, evident in several corruption and money laundering cases.

Although cryptocurrencies can be seized under law enforcement processes in Indonesia face difficulties handling them due to limited regulations on cryptocurrency seizure and lack of knowledge among law enforcement officers regarding their management. These new guidelines regulate various aspects of handling cryptocurrencies ranging from valuation assessments to procedures for seizure and storage of evidence within controlled crypto wallets. Three key principles must be observed during seizures: due process, transparency, and privacy protection to ensure accountability while safeguarding individual rights (Benson et al., 2024).

The process of seizing cryptocurrencies must be conducted carefully starting with tracing asset existence through coordination with relevant parties involved. Once identified steps toward seizure proceed according existing provisions handling evidence unconventional manner using secure ledger systems given volatility policy selling evidence declining value differs practices countries Germany.

In Indonesia legal arrangements concerning cybercrime-related cryptocurrency seizure remain relatively new unstructured despite recognition trading officially since 2016 acknowledgment commodity futures exchange Bappebti regulation governing seizure limited currently follows Criminal Procedure Code KUHAP doesn’t specifically address digital assets.

Under KUHAP seizure legal step requiring court chairman approval except urgent situations involves gathering suspected transaction information investigators coordinate Bappebti physical traders obtain wallet-related information perpetrators complex procedure requires deep understanding blockchain technology transaction mechanisms potential privacy issues users (Lukito 2019).

Attorney General’s Guidelines Number 7 of 2023 outlines principles handling cryptocurrency including due process transparency privacy aims accountability ensuring individual rights protected challenges knowledge enhancement law enforcement officers

developing specific regulations addressing unique aspects digital assets. In Indonesia cryptocurrency unrecognized official payment tool usage increases investment transaction Attorney General authority seize suspected illegal activities including crypto typically conducted laws regulating money laundering fraud Attorney General criminal laws seize case notable investment fraud platform individuals promising high returns unclear basis identifying seizing illegally obtained crypto involves investigation evidence submission court approval seized managed authorities proceedings emphasizes caution investors advised invest platforms registered regulated authorities Bappebti (Widyatmoko et al., 2024).

Additionally, supervision Financial Transaction Reports Analysis Center PPATK important handling crypto seizure PPATK analyzes suspicious transactions links parties involved despite challenges confidentiality blockchain technology Indonesian cases PT Asabri Indra Kenz demonstrate seizure possible procedures difficult highlights need clearer comprehensive legal framework addressing challenges cybercrime-related crypto asset seizure IDADX 2023.

4.2. Legal Solutions to Address Regulatory Gaps in Crypto Asset Seizure in Cybercrime Cases in Indonesia

Seizure in criminal procedure law means taking or holding an object, whether movable or immovable, belonging to a person or entity. This action is carried out by investigators to obtain evidence related to a criminal act and plays a crucial role in the process of proving a criminal case. The criminal justice process begins with an investigation by investigators, followed by prosecution by public prosecutors, trial examination, and execution of verdicts by prosecutors. Effective proof heavily depends on the presence of valid evidence (Watters, 2023).

It is essential to understand terms related to proof, such as evidence, proving, and proof itself. Evidence refers to anything that explains a particular fact, while proving is the process of presenting evidence to the judge. Proof involves procedures regulated by law to establish the defendant's guilt. In this context, proof in criminal law aims to seek material truth regarding legal events.

Seizure is considered an act that may contradict human rights because it involves taking a suspect's property. Therefore, seizure must be conducted in accordance with the applicable criminal procedure law. In Indonesia, seizure is regulated under Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP). The primary purpose of seizure is to obtain the necessary evidence in legal proceedings and to ensure that the evidence remains unchanged, which could affect proof (Toner, 2024).

Items that may be seized include objects used to commit a crime, proceeds of a crime, and other items relevant as evidence. Investigators, including the police and civil servant investigators (PPNS), have the authority to conduct seizures with permission from the head of the district court. The storage process for evidence is also strictly regulated to maintain its quality and integrity so that it can be effectively used in court proceedings (Puspasari, 2020).

Although cryptocurrency has become part of the global financial landscape, regulations regarding the seizure of cryptocurrency in criminal cases in Indonesia are still developing. There is no specific law explicitly governing the procedure for seizing cryptocurrency assets. However, several regulations and legal principles have been applied in the seizure process, including:

1) Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes (UU TPPU). This law serves as the primary legal framework for handling money laundering cases involving cryptocurrency. It regulates the tracking, freezing, and seizure of assets resulting from criminal activities, including cryptocurrency assets.

2) The Criminal Procedure Code (KUHAP). KUHAP regulates the general procedure for seizing evidence in criminal cases. Its provisions can be analogously applied to cryptocurrency asset seizures, despite some differences in characteristics between cryptocurrency and other physical evidence.
3) Regulations from the Commodity Futures Trading Supervisory Agency (BAPPEBTI). BAPPEBTI, as the regulator of cryptocurrency trading in Indonesia, has issued various regulations related to cryptocurrency transactions. These regulations can serve as references for identifying and tracking cryptocurrency assets.
4) Attorney General's Guidelines No. 7 of 2023. This guideline provides specific instructions for prosecutors in handling cryptocurrency assets as evidence in criminal cases. It covers the assessment of cryptocurrency asset value, seizure procedures, and storage of evidence in a controlled crypto wallet (Shodiq, 2023).

Although some regulations, such as UU TPPU and the Attorney General's Guidelines, address cryptocurrency assets in general, there is no specific Police Regulation (Perpol) detailing the procedure for seizing cryptocurrency assets by the Indonesian National Police (Polri). A Perpol is crucial in providing clear and uniform guidelines for all police officers in carrying out their duties. The absence of a Police Regulation on cryptocurrency asset seizures poses a significant challenge for law enforcement, especially in cybercrime cases. Therefore, Polri must initiate the drafting of a Perpol specifically governing cryptocurrency asset seizures. This Perpol should include the definition of cryptocurrency assets, seizure procedures, and legal treatment of these assets in the legal process. With a Perpol in place, law enforcement officers will have clear guidelines on handling cryptocurrency asset seizures (Alekseenko, 2023).

In drafting the Perpol, Polri needs to collaborate with relevant institutions, such as Bappebti, the Financial Transaction Reports and Analysis Center (PPATK), and the judiciary. This cooperation is essential to ensure that all technical and legal aspects of cryptocurrency asset seizure are understood and accommodated in the new regulation. Polri can also refer to best practices from other countries that have established clear regulations on cryptocurrency asset seizures. By studying and adapting policies and procedures proven effective elsewhere, Indonesia can accelerate the formulation of a Perpol that aligns with local conditions.

While awaiting an official Perpol, Polri can develop an interim internal guideline to provide direction for law enforcement officers in handling cryptocurrency asset seizures. This guideline could include procedural steps to be followed in seizing and managing cryptocurrency assets used as evidence.

To ensure the effective implementation of the Perpol and internal guidelines, training and education for Polri personnel on the basic concepts of cryptocurrency, blockchain technology, and appropriate seizure methods are necessary. Proper knowledge will enhance law enforcement effectiveness in handling cases involving cryptocurrency assets. After the Perpol is issued, monitoring and evaluation of its implementation should be conducted. Polri can periodically review whether the prescribed procedures are being followed and if any revisions or adjustments are needed based on technological developments and field practices.

Besides internalizing the regulation within Polri, public awareness campaigns on the new Perpol governing cryptocurrency asset seizures are also necessary. The public needs to understand the risks and legal responsibilities associated with cryptocurrency use and the regulations governing it (Gozali, 2020).

Addressing the regulatory gap in cryptocurrency asset seizures in cybercrime cases in Indonesia requires a comprehensive and integrated legal approach beyond merely issuing a Perpol. Some comprehensive legal solutions that can be implemented include:

1) Drafting a Special Regulation
   The government and legislative bodies need to promptly draft a regulation specifically governing aspects of cryptocurrency asset seizures. This regulation should cover the definition of cryptocurrency assets, seizure procedures, treatment of cryptocurrency as evidence, and mechanisms for storing and managing assets post-seizure. Clear regulations will provide law enforcement with a strong legal basis for carrying out seizures and minimize ambiguity in their implementation (Haji, 2022).
2) Strengthening the Existing Legal Framework
   Besides new regulations, it is necessary to strengthen the existing legal framework, such as UU TPPU and KUHAP. Adjustments and integration of provisions within these laws can help establish a more solid legal foundation for law enforcement related to cryptocurrency assets. For example, adding clauses specifically regulating the seizure of digital assets in money laundering and other criminal activities (Yanuar, 2022).
3) Developing Operational Guidelines for Law Enforcement
   To ensure effective regulatory implementation, clear operational guidelines for law enforcement officers are needed. These guidelines should detail practical steps in seizing cryptocurrency assets, including investigation procedures, transaction tracking, and coordination with institutions such as Bappebti and PPATK. This will help expedite investigations and improve accuracy in handling cryptocurrency assets involved in criminal acts.
4) Enhancing Human Resource Capacity
   Training and education for law enforcement on blockchain technology, cryptocurrency, and relevant investigative methods are essential. With adequate knowledge, law enforcement officers will be better equipped to handle cases involving cryptocurrency assets and understand the complexity of digital transactions. Training should also include ethical considerations and human rights principles in law enforcement against digital assets.
5) International Coordination
   Given the transnational nature of cryptocurrency assets, the Indonesian government needs to establish international cooperation in cybercrime law enforcement. By collaborating with other countries and international organizations, Indonesia can strengthen mechanisms for tracking and seizing cryptocurrency assets involved in cross-border crimes, including information exchange and best practices (Putri, 2021).
6) Public Awareness Campaigns
   In addition to legal measures, raising public awareness about cryptocurrency-related risks and the importance of complying with existing regulations is crucial. The public should understand that using cryptocurrency without proper knowledge could expose them to criminal liability. Education efforts can be conducted through various communication channels, such as seminars, media campaigns, and collaborations with digital asset communities (Bostwick et al., 2023).

The regulatory gap concerning cryptocurrency asset seizures is a serious challenge that must be addressed immediately. With comprehensive and effective regulations, law enforcement against cybercrime involving cryptocurrency assets can be carried out more

efficiently, while also providing legal certainty for businesses in the cryptocurrency sector and protecting public interests.

5. Conclusion

The seizure of crypto assets in cybercrime cases in Indonesia is still relatively new and faces many challenges. Although crypto assets are recognized as digital commodities that can be traded, the legal provisions governing their seizure remain limited and follow procedures outlined in the Indonesian Code of Criminal Procedure (KUHAP). Investigators must coordinate with the Commodity Futures Trading Regulatory Agency (Bappebti) and physical traders to gather information on suspicious transactions and obtain court approval for seizure. Attorney General's Guidelines No. 7 of 2023 have been issued to regulate the handling of crypto assets as evidence, emphasizing principles such as due process and transparency. However, challenges such as law enforcement officers' lack of understanding of blockchain technology and unclear regulations continue to hinder the effectiveness of the seizure process.

The absence of regulations on the seizure of crypto assets in cybercrime cases in Indonesia requires a comprehensive legal approach to strengthen law enforcement. Currently, although some relevant regulations exist, such as the Anti-Money Laundering Law (UU TPPU) and KUHAP, there is no specific regulation (Perpol) detailing the procedure for crypto asset seizure. Therefore, the National Police (Polri) and the government need to urgently draft regulations covering the definition, seizure procedures, and legal treatment of crypto assets. Additionally, strengthening the existing legal framework, developing operational guidelines for law enforcement, enhancing human resource capacity, international coordination, and educating the public about the risks of crypto assets are also crucial steps. With clear and comprehensive regulations, law enforcement can be more effective, providing legal certainty for businesses and protecting society from potential cybercrime risks.

Based on the explanation regarding the absence of regulations on crypto asset seizure and the challenges faced in law enforcement against cybercrime, some recommendations for the present and future include:

1) The National Police (Polri) can promptly issue temporary internal guidelines to regulate the procedure for seizing crypto assets, providing law enforcement officers with a reference for handling urgent cases.
2) Conducting intensive training for law enforcement personnel on crypto assets, blockchain technology, and proper seizure methods. This knowledge is essential to enhance the effectiveness of investigations.

6. References

Alekseenko, A. P. (2023). Model framework for consumer protection and crypto-exchanges regulation. *Journal of Risk and Financial Management, 16*(5), 305. https://doi.org/10.3390/jrfm16050305

Benson, V., Adamyk, B., Chinnaswamy, A., & Adamyk, O. (2024). Harmonising cryptocurrency regulation in Europe: Opportunities for preventing illicit transactions. *European Journal of Law and Economics*. https://doi.org/10.1007/s10657-024-09794-7

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., ... & Cloud, K. (2020). *Global cryptoasset regulatory landscape study. University of Cambridge Faculty of Law Research Paper (23)*. http://dx.doi.org/10.2139/ssrn.3379219

Bostwick, L., Bartlett, N., Cronje, H., & Abernathy III, T. J. (2024). Managing Seized and

Confiscated Assets-A Guide for Practitioners. *World Bank Publications-Books*.

Caianiello, M., & Camon, A. (2021). *Digital forensic evidence: Towards common European standards in antifraud administrative and criminal investigations*. OLAF.

Gozali, D. S. (2020). *Pengantar perbandingan sistem hukum (Civil Law, Common Law, dan Hukum Adat)*. Nusa Media.

Hafizhah, A., Baskoro, A., & Wahyuda, A. R. (2023). Regulating innovation: Addressing the potential threats of NFT and metaverse on intellectual property rights. *Indonesian Law Journal, 16*(2), 123–145.

Haji, R. (2022). Urgensi penerapan kerangka regulasi aset kripto yang komprehensif, adaptif, dan akomodatif. *Trade Policy Journal, 1*(Desember), 45–60.

Hidayat, R. (2021). 'Sudah Ikhlas': Banyaknya Kasus Penipuan Daring Tak Diproses Polisi. *Tirto.id*. https://tirto.id/sudah-ikhlas-banyaknya-kasus-penipuan-daring-tak-diproses-polisi-gk9r

IDADX. (2023, September 25). Serangan phishing di Indonesia terus meningkat, berikut data lengkapnya. *Bank Jombang*. https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya/

Kabra, S., & Gori, S. (2023). Drug trafficking on cryptomarkets and the role of organized crime group. *Journal of Economic Criminology, 2*, 100026. https://doi.org/10.1016/j.jeconc.2023.100026

Kristiani, E., Tsan, Y. T., Liu, P. Y., Yen, N. Y., & Yang, C. T. (2022). Binary and multi-class assessment of face mask classification on edge AI using CNN and transfer learning. *Human-centric Computing and Information Sciences*, *12*.

Lintasarta Cloudeka. (2023, September 25). 5 contoh phishing yang harus diwaspadai. *Cloudeka*. https://www.cloudeka.id/id/berita/web-sec/contoh-phising/

Lukito, R. (2019). *Perbandingan hukum*. UGM Press.

Puspasari, S. (2020). Perlindungan hukum bagi investor pada transaksi aset kripto dalam bursa berjangka komoditi. *Jurist-Diction, 3*(1), 305–320.

Putri, K. V. K. (2021). Kerja sama Indonesia dengan ASEAN mengenai cyber security dan cyber resilience dalam mengatasi cyber crime. *Rewang Rencang: Jurnal Hukum Lex Generalis, 2*(7), 45–60.

Rahardjo, S. (2008). *Membedah hukum progresif*. Kompas.

Reedy, P. (2024). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy, 6*, 100313. https://doi.org/10.1016/j.fsisyn.2023.100313

Rosales, A., van Roekel, E., Howson, P., & Kanters, C. (2023). Poor miners and empty e-wallets: Latin American experiences with cryptocurrencies in crisis. *Human Geography*, 1–12. https://doi.org/10.1177/19427786231152934

Shodiq, M. D. (2023). *Perbandingan sistem hukum*. PT Mafy Media Literasi Indonesia.

Soekanto, S. (2007). *Sosiologi suatu pengantar*. Rajawali Press.

Suhartanto, C. (2024, March 18). RI peringkat ketiga, negara dengan serangan phishing terbanyak di ASEAN 2023. *Bisnis*. https://teknologi.bisnis.com/read/20240318/84/1750246/ri-peringkat-ketiga-negara-dengan-serangan-phising-terbanyak-di-asean-2023

Syamsu, N., Sofyan, S., Aisya, S., & MD, M. (2022). Integration of Using Fintech and Social Media for The Business Sustainability in Pesantren. *EKONOMIKA SYARIAH: Journal of Economic Studies*, *6*(2), 167.

Toner, D. (2024). *Human rights review of privacy and policing*. Northern Ireland Policing Board.

U.S. Department of Treasury. 2022. *Crypto-Assets: Implications for Consumers, Investors, and Businesses*. E-Book.

Watters, C. (2023). When criminals abuse the blockchain: Establishing personal jurisdiction

in a decentralised environment. *Laws, 12*(2), 33. https://doi.org/10.3390/laws12020033

Widyatmoko, U., Atmasasmita, R., Susanto, A. F., & Purwanto, B. H. (2024). Law enforcement against cryptocurrency abuse. *Journal of Social Research, 3*(2), 123–135.

Yanuar, M. A. (2022). Risiko dan posibilitas penyalahgunaan aset kripto dalam kejahatan pencucian uang. *Majalah Hukum Nasional, 52*(2), 123–145.

Yanwardhana, E. (2024). Gaya penipuan baru 2024 di WA dan email, rekening dikuras habis. *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20240302164346-37-519138/gaya-penipuan-baru-2024-di-wa-dan-email-rekening-dikuras-habis