Majelis: Jurnal Hukum Indonesia
Volume 2, Nomor 3, Agustus 2025
e-ISSN: 3063-3826; p-ISSN: 3063-380X, Hal. 105-125
DOI: https://doi.org/10.62383/majelis.v2i3.1042
Available Online at: https://ejournal.appihi.or.id/index.php/Majelis

Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, And Legal Voids in the Criminal Law System in Indonesia

Pambudi[1*], Zudan Arief Fakrulloh[2]
[1,2] Universitas Borobudur,Indonesia
pambudi.indag1996@gmail.com[1*], cclsis@yahoo.com[2]

Korespondensi penulis: pambudi.indag1996@gmail.com

Abstract*. This study aims to examine the legal gaps and regulatory challenges in enforcing criminal liability against perpetrators of crimes within Indonesia's crypto ecosystem, particularly in the context of Decentralized Finance (DeFi), smart contracts, and decentralized digital asset trading platforms. The research employs a normative juridical approach using statutory and conceptual methods. The findings indicate that current criminal law instruments, such as Article 378 of the Criminal Code, Article 28 paragraph (1) of the Electronic Information and Transactions (ITE) Law, Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU), and Law No. 10 of 1998 on Banking, are inadequate to address the unique and complex characteristics of crypto-related crimes. These crimes are anonymous, cross-jurisdictional, and difficult to trace due to the absence of centralized authority. As a result, the existing legal framework fails to provide sufficient victim protection and leads to weak law enforcement effectiveness. This legal vacuum also hampers the state's ability to respond to the growing digital threats and creates legal uncertainty in the expanding crypto space. Therefore, this study recommends the formulation of specific criminal regulations that comprehensively define digital assets, legal subjects within decentralized systems, and new criminal offenses relevant to crypto-related conduct. It also calls for the establishment of specialized institutions dedicated to investigating and prosecuting such crimes. These proposed regulations are expected to strengthen the national criminal justice system, making it more adaptive, fair, and effective in addressing the challenges posed by digital transformation.*

Keywords*: Blockchain, Criminal Liability, Crypto Crime, Legal Vacancy*

Abstrak. Penelitian ini bertujuan untuk mengkaji kesenjangan hukum dan tantangan regulasi dalam penegakan pertanggungjawaban pidana terhadap pelaku kejahatan dalam ekosistem kripto Indonesia, khususnya dalam konteks Keuangan Terdesentralisasi (DeFi), kontrak pintar, dan platform perdagangan aset digital terdesentralisasi. Penelitian ini menggunakan pendekatan yuridis normatif dengan metode perundang-undangan dan konseptual. Temuan penelitian menunjukkan bahwa instrumen hukum pidana yang ada saat ini, seperti Pasal 378 KUHP, Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (ITE), Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU), dan Undang-Undang No. 10 Tahun 1998 tentang Perbankan, belum memadai untuk mengatasi karakteristik kejahatan kripto yang unik dan kompleks. Kejahatan ini bersifat anonim, lintas yurisdiksi, dan sulit dilacak karena tidak adanya otoritas terpusat. Akibatnya, kerangka hukum yang ada gagal memberikan perlindungan korban yang memadai dan menyebabkan lemahnya efektivitas penegakan hukum. Kekosongan hukum ini juga menghambat kemampuan negara untuk merespons ancaman digital yang terus berkembang dan menciptakan ketidakpastian hukum di dunia kripto yang terus berkembang. Oleh karena itu, studi ini merekomendasikan perumusan peraturan pidana khusus yang secara komprehensif mendefinisikan aset digital, subjek hukum dalam sistem terdesentralisasi, dan tindak pidana baru yang relevan dengan perilaku terkait kripto. Studi ini juga menyerukan pembentukan lembaga khusus yang didedikasikan untuk menyelidiki dan menuntut kejahatan semacam itu. Peraturan yang diusulkan ini diharapkan dapat memperkuat sistem peradilan pidana nasional, menjadikannya lebih adaptif, adil, dan efektif dalam mengatasi tantangan yang ditimbulkan oleh transformasi digital.

Kata Kunci: Blockchain, Kejahatan Kripto, Kekosongan Hukum, Tanggung Jawab Pidana

Received: Juli 15, 2025; Revised: Juli 29, 2025; Accepted: Juli 30, 2025; Published : Agustus 01, 2025

1 INTRODUCTION

The development of blockchain technology since its introduction through Bitcoin in 2009 has brought a major revolution in the world of digital finance and various other sectors. Blockchain, as a decentralized and encrypted transaction recording system, allows the creation of crypto assets that are not controlled by a single authority (Arwani, 2024). Over time, the crypto ecosystem has grown rapidly with the emergence of thousands of new types of digital assets, each offering different features and uses, such as Ethereum which introduced the concept of smart contracts to run automatic programs without human intervention. In addition, the birth of various innovations such as Non-Fungible Tokens (NFT) which represent digital ownership of unique assets, and Decentralized Finance (DeFi) which offers financial services without traditional intermediaries such as banks, have expanded the scope of blockchain far beyond just a medium of value exchange (Lestari, 2024). Digital asset trading platforms such as Binance, Uniswap, and OpenSea have become global transaction centers that can be accessed by anyone with an internet connection, removing many geographical and bureaucratic boundaries in financial transactions. This ecosystem is growing quickly and is increasingly complex, creating a new economic order based on decentralization that is not yet fully regulated in the conventional legal system (Martinelli, 2024).

In Indonesia, the adoption of crypto technology and digital assets has shown significant growth, driven by increasing internet penetration, digital financial literacy, and the attractiveness of high investment returns. This phenomenon has brought broad socio-economic impacts, including the creation of new jobs in the financial technology (fintech) sector, investment opportunities for the wider community, and the development of the creative industry sector through NFT and asset tokenization (Astrawan, 2021). However, on the other hand, this technology also poses serious legal challenges, especially related to consumer protection, supervision of financial transactions, and criminal liability for crimes that occur in the decentralized digital realm. The Indonesian criminal law system, which is based on a traditional approach to legal subjects and locus delicti (place of the crime), faces great difficulty in accommodating the unique characteristics of the crypto ecosystem (Darmawan, 2020). The inability to establish a clear legal subject in DeFi transactions, the complexity of ensnaring criminals behind anonymous smart contracts, and the difficulty of enforcing the law against perpetrators operating on cross-border platforms require legal reforms are more adaptive to this new reality.

The open, blockchain-based crypto ecosystem creates great opportunities not only for financial innovation but also for the birth of various new, complex forms of crime (Wijaya,

2016). One of the most common forms of crime is fraud, including rug pull schemes, which is a mode in which crypto project developers suddenly withdraw all investor funds and disappear without a trace. In addition, money laundering practices are also rampant through crypto assets, where criminals take advantage of the anonymity and difficulty of tracking in the blockchain to obscure the origin of illegal funds. Phishing or fraud through social engineering techniques to steal private keys or user account information is also a crime that often claims many victims. No less important, theft of digital assets through hacking of crypto wallets or attacks on crypto exchanges is a serious threat, with losses sometimes reaching billions of dollars in a single incident (Ilyasa, 2019). Another form of crime is crypto market manipulation, such as pump and dump schemes, where the price of a digital asset is artificially inflated and then sold at a peak price, harming small investors who are deceived by the false price increase.

The main characteristic of crimes in the crypto ecosystem is their anonymous, cross-border nature, and they are very difficult to trace using conventional investigative methods. Blockchain technology does store all transactions publicly and permanently, but the identities of the perpetrators behind the digital wallet addresses are often hidden or disguised using techniques such as mixing services or privacy coins, making it difficult to link transactions to real identities. In addition, because crypto transactions are global and do not recognize national jurisdictional boundaries, perpetrators can operate from anywhere in the world, making law enforcement in one country less effective without strong international cooperation (Noorsanti, 2018). These characteristics create new challenges for law enforcement officers, both in terms of proving criminal acts, tracking the flow of funds, and determining who can be asked for criminal liability. In a legal environment that still relies on traditional concepts of jurisdictional scope and clear legal subjects, crypto crimes demonstrate the urgent need for criminal regulatory reform that is more adaptive to the decentralized and borderless digital world. (Rahmanto, 2020)

In the Indonesian legal system, efforts to prosecute criminals in the crypto ecosystem still rely on laws and regulations originally designed for conventional crime contexts. One of the main examples is the use of Article 378 of the Criminal Code (KUHP) which regulates the crime of fraud. This article criminalizes fraudulent acts with deception to benefit oneself or others unlawfully (Razzaq, 2018). However, in crypto, the modus operandi of crimes such as rug pull schemes, the creation of fake tokens, or the misuse of smart contracts often do not meet the classical elements of deception or lies required in this article. Crimes in the crypto realm are more technical and systemic, using algorithms or smart contract loopholes, making it difficult to qualify as fraud in the traditional sense of Article 378 of the Criminal Code. As a

result, many perpetrators cannot be effectively prosecuted, even when they have harmed the victim (Rinaldi, 2016).

Article 28 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is also often used as a legal basis to ensnare digital criminals, including in the crypto ecosystem. This article regulates the prohibition of the dissemination of misleading information that is detrimental to consumers in electronic transactions. However, the phrase "misleading information" in this provision creates ambiguity in its implementation against crypto crimes. For example, in the case of a token project promotion that turns out to end in a rug pull, it is difficult to prove whether the information disseminated from the start has met the elements of misleading or is a change of intention after the funds have been collected (Rohman, 2021). This unclear limitation causes legal uncertainty in the criminal enforcement process against perpetrators of digital asset-based fraud.

Furthermore, money laundering through crypto assets, there is a lack of specific regulations in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (UU TPPU). This law generally regulates efforts to prevent and eradicate money laundering through various forms of assets but has not explicitly listed blockchain-based digital assets such as crypto as objects of crime. In addition, the anonymous, fast, and cross-border characteristics of crypto transactions make it difficult for supervisory and law enforcement agencies to track the flow of funds from crime (Sajidin, 2021). Although the basic principles of the TPPU Law can be interpreted broadly, the absence of explicit regulations regarding crypto in the list of assets or types of transactions that are supervised creates legal loopholes that are exploited by criminals. In the financial sector, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (Banking Law) also shows its limitations. The articles regulating fundraising activities and payment services, especially Articles 46 to 50B, only cover transactions through the state-supervised banking system. Stablecoins and other digital assets that function as a means of payment outside the national banking authority are not accommodated in this provision. This means that the use of digital assets as a means of payment, although potentially threatening the stability of the financial system, cannot be directly categorized as a violation based on the existing Banking Law (Budiman, 2020). Banking regulations based on the assumption of centralization and state supervision are ineffective in dealing with decentralized and community-based payment asset innovations.

One of the main challenges in enforcing criminal law against crimes in the crypto ecosystem is the lack of clarity regarding the legal subject responsible. In traditional systems, legal subjects are usually individuals or legal entities that can be identified and are subject to state jurisdiction (Herlambang, 2020). However, in the context of blockchain and DeFi technology, many platforms operate decentralized without a single central entity that can be held accountable. Smart contracts that run automatically without human intervention, decentralized autonomous organizations (DAOs) managed by anonymous global communities, and non-custodial digital asset exchanges create situations where it is very difficult to determine who should be held legally responsible when a crime or loss occurs (Rahayu, 2021). This condition causes many criminals in the crypto ecosystem to hide behind the system anonymity and avoid legal accountability.

The absence of specific regulations governing criminal liability in the context of crypto and DeFi exacerbates the problem. Currently, Indonesia still relies on general regulations that are not designed to deal with the new realities of decentralized technology. There are no positive legal provisions that explicitly stipulate how to classify perpetrators in DeFi transactions, or how to establish legal responsibility for algorithms or protocols that are the means by which criminal acts occur. As a result, the scope of criminal law becomes blurred when faced with crimes that do not have directly identifiable human perpetrators or are taken out collectively by anonymous entities across countries (Purwanto, 2021). This creates a legal vacuum that opens up loopholes of impunity for perpetrators of crimes in the digital world.

In addition, the lack of adequate legal instruments to ensnare perpetrators on non-traditional platforms further weakens the effectiveness of criminal law enforcement. Blockchain-based peer-to-peer lending platforms, decentralized exchanges (DEX), and NFT marketplaces are not regulated by conventional financial law making it difficult for law enforcement officers to conduct investigations, provide evidence, and enforce the law (Chong, 2022). Without formal registration mechanisms, user identification, or legal compliance requirements, criminals can easily exploit this system to commit fraud, money laundering, or other crimes without much risk of being caught. The absence of specific instruments such as provisions on digital identity obligations, reporting suspicious transactions based on digital assets, or provisions on the accountability of smart contract operators makes the existing criminal law system irrelevant to the increasingly complex and rapidly changing digital world.

Given these challenges, criminal regulatory reform in the digital era is urgent. The legal vacuum not only weakens the effectiveness of law enforcement but also sacrifices the protection of the rights of victims of digital crime who often lose high-value assets without any

guarantee of recovery. Without a clear legal framework, law enforcement officers are in a difficult position to process cases, while criminals are increasingly daring to use technology to carry out their actions. Therefore, a criminal law policy must be adaptive to technological changes, able to accommodate the characteristics of digital assets and provide an effective and enforceable accountability mechanism across jurisdictions. This research aims to contribute to drafting more comprehensive and responsive regulations, to ensure that the crypto ecosystem in Indonesia can develop healthily and remain within the legal corridor that provides maximum protection for all parties involved.

2 METHOD

This study uses a normative legal method, namely legal research conducted by examining primary and secondary legal materials through a statutory approach and a conceptual approach. The statutory approach is used to analyze applicable laws and regulations related to crimes in the crypto ecosystem and their criminal liability, while the conceptual approach is used to understand the concept of criminal liability in the context of digital technology and decentralization. Data sources in this study include primary legal materials, such as the Criminal Code (KUHP), the Law on Information and Electronic Transactions, the Law on the Prevention and Eradication of Money Laundering, and other relevant regulations, and secondary legal materials in the form of literature, legal journals, scientific articles, and opinions of legal experts. Data collection techniques are carried out through library research by collecting, reading, and reviewing legal documents and related literature. The data analysis technique used is qualitative analysis by interpreting laws and regulations, comparing existing legal concepts, and examining the suitability and legal gaps that occur in practice to formulate adaptive legal solutions to the development of crypto technology in Indonesia.

3 RESULT AND DISCUSSION

Current Criminal Law Regulations in Indonesia Regarding the Accountability of Criminals in the Crypto Ecosystem

The basic principle of criminal liability in Indonesia refers to the principle of *nullum delictum sine lege*, which means that no act can be punished without a legal provision that regulates it. In the Indonesian criminal law system, every individual who commits an act that is prohibited by law and harms others or society can be held criminally responsible. The concept of criminal liability consists of two main elements, namely the existence of an unlawful act (actus reus) and the intent or fault (mens rea) of the perpetrator. Criminal law in Indonesia

is retributive and corrective, namely aiming to provide punishment that is commensurate with the perpetrator's actions and to provide a deterrent effect so that society complies with applicable laws. However, for crimes that occur in the crypto ecosystem, the application of these principles is not easy, because the nature of technology-based crimes is very different from conventional crimes (Buckley, 2020).

The Criminal Code (KUHP) as Indonesia's general criminal law is based on regulations regarding crimes committed by individuals or groups whose identities are clear and within a recognizable scope. In the case of crypto crimes, such as fraud committed through digital asset exchange platforms or smart contract-based transactions, the application of the Criminal Code cannot be directly adapted. Articles in the Criminal Code such as Article 378 which regulates fraud do not explicitly accommodate forms of fraud involving decentralized digital technology, without a managing entity or one that can be held directly responsible. For example, in a rug pull scheme on a crypto platform, it is difficult to identify who should be held criminally responsible, because no party or individual can be directly responsible for the losses incurred (Tauda, 2023).

The limitations of classical legal principles in dealing with decentralized technology-based crimes are visible in the problem of identifying legal subjects and jurisdiction. Crimes in the crypto ecosystem, especially those that occur on Decentralized Finance (DeFi) platforms or the use of smart contracts, are often committed by individuals or groups whose identities cannot be known with certainty, given that blockchain technology offers anonymity and does not depend on a centralized manager. In addition, the decentralized nature of many crypto platforms means that transactions can occur without involving a third party that can be supervised by conventional law. As a result, even though the losses incurred are very real, law enforcement referring to the classical approach in the Criminal Code becomes very difficult, because there is no individual or legal entity that can be directly held responsible.

The use of Article 378 of the Criminal Code for digital asset-based fraud faces major challenges in the context of the crypto ecosystem. This article regulates the crime of fraud committed by tricking someone into handing over goods or money with false promises. However, in cases of crypto-based fraud, such as fraud that occurs on digital asset trading platforms or crypto-based investments, the application of Article 378 of the Criminal Code is often inappropriate. This is due to the anonymous and decentralized nature of crypto transactions, making it difficult to prove malicious intent (mens rea) or a clear form of fraud in transactions involving multiple parties or even automated systems through smart contracts. Therefore, although Article 378 of the Criminal Code can be used for cases of fraud that occur

in crypto, its application is very limited and often requires a more flexible legal interpretation to accommodate forms of fraud that are not found in traditional transactions.

Application of Article 28 paragraph (1) of Law No. 1 of 2024 concerning Amendments to Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) provides a more relevant legal basis in dealing with fraud or the spread of misleading information in the crypto world. This article regulates the prohibition of spreading information that can harm other parties, including information that can deceive or confuse the public. In crypto, this article can be used to ensnare perpetrators who commit fraud, such as in the case of rug pulls or fraudulent investment schemes that offer fake digital assets. However, this article still has ambiguity, especially in regulating the phrase "misleading information," which in practice is often difficult to prove. For example, in the crypto world, the difference between legitimate crypto project promotions and fraudulent schemes is often blurred, due to the many claims circulating on digital platforms that are not regulated. Therefore, although Article 28 paragraph (1) of the ITE Law can be used, this regulation still requires clarification and further development so it is effective in dealing with crypto crimes.

Law No. 8 of 2010 concerning Money Laundering Crimes (UU TPPU) provides a legal basis for tackling money laundering using digital assets, but its implementation also faces significant difficulties. The anonymous and decentralized nature of crypto makes it extremely difficult to track the flow of laundered money. Articles in the TPPU Law require the identification of suspicious transactions and the obligation to report large or suspicious transactions to the authorities. However, in crypto, where the identities of users and perpetrators are often not revealed due to the pseudonymous nature of blockchain technology, it is difficult to link transactions to the identities of the actual perpetrators. In addition, crypto transactions that are decentralized and peer-to-peer platforms make tracking and proof even more difficult, so many transactions are at risk of escaping supervision. Therefore, although the TPPU Law can be applied in the context of crypto, its use must be accompanied by adaptations to the specific challenges faced by blockchain technology and digital assets.

Law No. 10 of 1998 concerning Banking, specifically Articles 46 to 50B, regulates the prohibition of the transfer or use of unauthorized payment instruments. Although this regulation focuses on the supervision of the conventional banking system, it does not specifically accommodate transactions involving crypto or stablecoins as legal or illegal payment instruments. With the growing use of crypto as a means of payment outside the financial system supervised by the state, it is increasingly clear that the articles in the Banking Law do not cover important aspects of the crypto ecosystem. For example, transactions using

stablecoins or other crypto as a means of payment outside the authority of Bank Indonesia and the Financial Services Authority (OJK) cannot be subject to sanctions in accordance with existing provisions. Thus, the limitations of Law No. 10 of 1998 concerning Banking are becoming increasingly apparent, and new regulations are needed that are more specific and relevant in regulating the use of crypto and stablecoins as legal tender in Indonesia.

The Commodity Futures Trading Supervisory Agency (BAPPEBTI) has an important role in regulating crypto asset trading in Indonesia. BAPPEBTI functions to ensure that digital asset transactions, such as Bitcoin, Ethereum, and other assets, are carried out in accordance with the rules applicable in the futures market. Since 2018, BAPPEBTI has designated crypto assets as commodities that can be traded on registered futures exchanges. In its efforts to regulate crypto asset trading, BAPPEBTI also grants licenses to crypto exchanges that are allowed to operate in Indonesia and supervise transactions so that they do not involve practices that are detrimental to consumers, such as fraud or market manipulation. However, although BAPPEBTI has the authority to regulate digital asset trading, its role is still limited to the trading aspect and does not yet cover all aspects of the crypto ecosystem, including the use of crypto in Decentralized Finance (DeFi) platforms and decentralized peer-to-peer transactions. It constructs a gap in supervision that can be exploited by irresponsible parties.

Meanwhile, Bank Indonesia (BI) and the Financial Services Authority (OJK) also play an important role in supervising the financial sector in Indonesia, but they face limitations in supervising the crypto sector. BI has issued a ban on the use of crypto assets as legal tender, but this does not prevent the use of crypto as an investment or speculative asset. On the other hand, OJK, as an institution that oversees the capital market and banking sector, does not have direct authority to supervise crypto asset transactions conducted outside the traditional financial system. The ambiguity about who has the authority to regulate crypto transactions has led to overlapping authority between institutions, while many crypto transactions occur outside the scope of supervision of the two institutions. This limited supervision creates legal loopholes that can be exploited to commit crimes like fraud, money laundering, and even terrorism financing involving digital assets.

In addition, the absence of a specific criminal framework for DeFi platforms and peer-to-peer transactions is a major challenge in law enforcement against crypto crimes. DeFi platforms and peer-to-peer transactions, which operate without a central authority, cannot be easily subject to criminal sanctions, because no party can be identified as the manager or perpetrator responsible. Even if there is a case of fraud or loss that occurs, it is difficult to determine who should be held accountable. This is exacerbated by the fact that DeFi and peer-

to-peer transactions are anonymous and difficult to track by conventional legal authorities. Therefore, to deal with crimes in this ecosystem, Indonesia needs more specific regulations that can regulate supervision and criminal liability in crypto transactions, including on DeFi platforms and transactions that occur between individuals directly without the intermediary of a centralized institution.

One of the main weaknesses of the existing legal regulations is the inability of existing articles to accommodate the anonymous and decentralized nature of crypto transactions. Crypto and blockchain technology, which are its basis, allow transactions to occur without involving a centralized third party and provide a high level of anonymity for users. This is contrary to the basic principles of criminal law which tend to rely on clear identification of perpetrators to establish criminal liability. For example, in fraud or money laundering using crypto, it is difficult to trace the identity of the perpetrators, because they can use digital wallets that do not require personal information. Articles in the Criminal Code or the ITE Law that focus on individual identification and third-party involvement cannot be easily applied to crypto transactions, which often occur anonymously and without verified intermediaries. As a result, many crimes in the crypto ecosystem are difficult to process legally, even though the losses incurred are real and large.

The next challenge is the difficulty in determining the legal subject in the Decentralized Finance (DeFi) ecosystem and the use of smart contracts. DeFi platforms, which operate without an identifiable central entity, as well as smart contracts that run automatically based on pre-programmed code, do not provide room for determining who can be held accountable if a crime occurs. In a traditional system, legal subjects such as individuals or companies that manage the system can be prosecuted. However, in the DeFi system, transactions and contract execution are carried out by code and not by parties who can be directly responsible. It creates confusion about who should be sued if losses occur due to system failure or fraud. Thus, without clear regulations regarding who is responsible, perpetrators of crimes can often avoid the clutches of the law, while victims lose their right to compensation or protection.

Jurisdictional barriers are another significant issue in tackling transnational crimes involving crypto. Most crypto transactions occur in a global digital space that is not bound by national borders, making it difficult to determine which country's law has jurisdiction over the actions of the perpetrator. Crypto enables transactions between countries without clear borders, making it difficult to apply the laws of a particular country. For example, if a perpetrator commits fraud through a DeFi platform that operates globally, how can the victim country hold the perpetrator accountable if the perpetrator is located in a country that does not have adequate

regulations or international cooperation to prosecute the crime? In addition, the existence of technologies that allow users to hide their identity and location, such as through the use of VPNs or masked IP addresses, makes law enforcement even more complicated.

Legal Impact of Regulatory Vacancies on Victim Protection and the Effectiveness of Criminal Law Enforcement in Crime Cases Involving Blockchain-Based Digital Assets

Legal protection for victims of crypto crime faces significant challenges due to the lack of existing regulations. Without clear and specific regulations regarding crimes involving blockchain-based digital assets, victims are often trapped in legal uncertainty. For example, in cases of fraud through crypto platforms or rug pull schemes, victims have difficulty obtaining compensation because there is no clear legal guarantee for their protection. Although many victims suffer significant financial losses, existing regulations do not provide certainty about who is responsible or how they can effectively claim their rights. Therefore, this lack of regulation leads to the inability of victims to obtain adequate legal protection, and their rights are often not recognized or protected by the existing legal system. Another major challenge is the difficulty in obtaining compensation or restitution for victims, given the limitations of the applicable laws. In the crypto world, transactions are often carried out anonymously, and criminals can move or hide assets involved in the crime. It makes it difficult to trace the flow of assets that have been stolen or used for illegal activities. In the existing criminal justice system, proving the existence or flow of these assets requires solid evidence, which is often difficult to obtain, especially when transactions are carried out using technology that is not fully understood by law enforcement. Without clear regulations regarding victim protection, they not only face difficulties in obtaining restitution but also in knowing whether they can claim damages or compensation for the losses they have suffered.

The difficulty in resolving disputes and providing justice to victims is exacerbated in a decentralized and anonymous ecosystem. In traditional systems, disputes can be resolved through the courts by presenting a responsible party, such as an individual or a company. However, in DeFi platforms or peer-to-peer transactions, there is no clear party responsible because the platform operates without a centralized governing entity. For example, in cases of fraud that occur on decentralized crypto exchanges, the perpetrator can simply disappear without a trace, leaving victims with no clarity about who to hold accountable. On the other hand, in other cases involving smart contracts, it is difficult to blame a specific party because the execution of the contract is carried out automatically based on code, not human decisions. As a result, many victims feel they have no way to seek justice or adequate dispute resolution.

The unclear protection framework for investors and users of crypto platforms in the context of applicable laws also worsens this situation. In Indonesia, although BAPPEBTI has set several regulations regarding crypto asset trading, legal protection for investors and users involved in the crypto ecosystem is still limited. Meanwhile, the use of crypto as an investment instrument or financial transaction that is not tied to the traditional banking system makes investors and users vulnerable to the risk of fraud and crime. Users of DeFi platforms or peer-to-peer transactions often do not have sufficient legal protection guarantees, considering that these transactions occur outside the supervision of regulated financial institutions. In the absence of clear regulations, investors who experience losses due to fraud or system errors in crypto platforms often do not have clear legal channels to report their cases or seek compensation.

The legal vacuum in the regulation related to crypto crimes has a significant impact on criminal enforcement, especially in cases of fraud, money laundering, and various other crimes that occur in the crypto world. Without clear and firm regulations regarding crimes involving blockchain-based digital assets, law enforcement officers have difficulty following up on these cases. For example, in cases of crypto-based fraud, such as rug pull or pump-and-dump schemes, perpetrators often use platforms or technologies that allow them to hide their identities and locations. As a result, victims may suffer significant losses, but the legal process to prosecute perpetrators becomes very complex. Furthermore, in the context of money laundering involving digital assets, the anonymity of blockchain makes it difficult for authorities to trace illegal transactions and identify the parties involved. This legal vacuum creates uncertainty for victims and worsens efforts to enforce effective criminal law against crypto crime.

Another challenge lies in the limited regulation of decentralized transactions, such as those on DeFi (Decentralized Finance) platforms. DeFi platforms operate without a centralized governing entity, making them unsupervised in the same way as traditional crypto exchanges that have clear authority. Transactions in the DeFi ecosystem are also often automated and do not involve a third party that can be identified or held accountable. This exacerbates the regulatory vacuum because there is no legal entity that can be involved in investigations or prosecutions. Unlike transactions that occur in a centralized financial system, which involve institutions that can be supervised and regulated, DeFi transactions are very difficult to monitor, triggering major difficulties in law enforcement related to crimes that occur on these platforms. Even in cases of cybercrime involving DeFi platforms, law enforcement becomes very complicated because no party can be held accountable for the incident.

The obstacle in determining the legal entity that can be held criminally responsible in cases of blockchain-based crimes is also a major obstacle to law enforcement. In the traditional criminal law system, the prosecution can identify the individual or entity responsible for a crime. However, in the crypto world, many transactions are conducted without identifiable identities, and criminals can even use technologies such as VPNs, anonymous wallets, or decentralized networks to hide their tracks. This makes it difficult for law enforcement to determine who can be held criminally accountable, especially when crimes occur on decentralized platforms or when perpetrators use smart contracts that run automatically based on code without human control. For example, in cases of fraud or embezzlement involving crypto assets, even when the loss is very clear, the legal process is hampered by the lack of mechanisms that can effectively identify the perpetrators.

The decreased effectiveness of law enforcement agencies in identifying, tracking, and prosecuting criminals involved in crypto-based transactions is also a serious impact of this legal vacuum. In Indonesia, although BAPPEBTI and other institutions are trying to supervise crypto asset trading, supervision of crimes involving digital assets outside of registered crypto exchanges is very limited. Authorities such as the police or other supervisory agencies often do not have sufficient understanding or technical capabilities to track anonymous and decentralized blockchain-based transactions. This worsens law enforcement efforts against criminals who exploit legal loopholes to operate without fear. Lack of training and knowledge related to blockchain technology and digital assets among law enforcement officers makes it difficult for them to utilize existing tools and resources to track perpetrators, identify evidence, and bring them to justice.

The inconsistency between the traditional criminal law system and the development of crypto technology is one of the fundamental problems in dealing with modern cybercrime. Traditional criminal law in Indonesia still relies heavily on principles that assume the existence of physically identifiable perpetrators, clear jurisdictional areas, and real and visible actions. However, in the crypto world based on blockchain technology and decentralized systems, perpetrators often hide their identities through anonymous digital wallets, virtual private networks (VPNs), and cross-border transactions that cannot be easily unraveled by legal authorities. It makes it impossible for conventional legal instruments, such as the Criminal Code or other laws that are still based on territorial approaches and personification of the perpetrators, to fully address crypto-based criminal cases. As a result, many crimes in the crypto ecosystem escape the law because our legal system is not designed to handle these types of modes.

Furthermore, the lack of adequate legal instruments to reach criminals who use technology to hide their tracks worsens the situation. In traditional systems, identifying the perpetrator is key to establishing criminal liability. However, in blockchain technology, criminals can operate using anonymous wallet addresses, avoid identity verification (Know Your Customer/KYC), and use DeFi protocols that do not require third-party involvement. The investigation mechanisms that law enforcement agencies of current punishments are not fully capable of reaching or dismantling this complex technological system. For example, when the proceeds of crime are transferred into mixing or tumbling protocols that disguise the origin of the funds, the tracking process becomes almost impossible without special tools and international cooperation. Therefore, new legal instruments are needed that explicitly regulate the methods of identifying perpetrators in this sophisticated digital context, including approaches to collective responsibility, pseudonymity, and the involvement of automated technologies such as smart contracts.

The major challenge in formulating regulations that are adaptive and responsive to crypto and blockchain technology lies not only in the speed of technological development, but also in the need to maintain a balance between legal certainty, public protection, and freedom of innovation. Regulations that are rigid and do not follow the dynamics of technology risk becoming irrelevant, while regulations that are too loose open up space for abuse. This requires policymakers and lawmakers to have an adequate understanding of technology to formulate legal norms that can answer today's challenges. In addition, there needs to be cross-sectoral cooperation, both nationally and internationally, so that the resulting regulations are not only effective at the domestic level but can also reach crimes that cross state jurisdictions. To that end, the drafting of new criminal laws, particularly those targeting crypto and digital asset crimes, must take into account the architecture of the technology itself, as well as provide a flexible approach and robust forensic technology for effective law enforcement.

An Ideal Draft of Regulations to Address Legal Gaps and Clarify Criminal Liability for Criminals in the Crypto Ecosystem in Indonesia

The urgency of establishing special regulations regarding crypto crimes is becoming increasingly urgent as the complexity and frequency of criminal acts occurring in the digital asset ecosystem increases. Crypto is not just an investment tool but has developed into a new medium for various financial activities, including illegal ones such as fraud (scams), rug pull schemes, money laundering, and digital wallet hacking. Unfortunately, the current criminal regulations are still oriented toward conventional crimes and do not specifically regulate new

forms of digital crimes that are decentralized, anonymous, and cross-jurisdictional. The absence of explicit legal norms creates uncertainty in the law enforcement process, makes it difficult for law enforcement officers to determine criminal elements, and has a direct impact on legal protection for the community. This shows that a reactive and partial legal approach is no longer adequate to address the dynamics of the crypto ecosystem which is developing rapidly and is not bound by traditional geographical boundaries.

In addition, the weaknesses of current regulations, such as the use of Article 378 of the Criminal Code to ensnare crypto fraud perpetrators or Article 28 paragraph (1) of the ITE Law to prosecute misleading information on digital asset platforms, show an imbalance between the characteristics of the crimes faced and the legal instruments used. This inaccuracy not only creates the potential for criminal misclassification but also violates the principle of legality in criminal law which demands legal certainty. Therefore, there needs to be harmonization between the national criminal law system and the unique characteristics of blockchain technology, smart contracts, and Decentralized Finance (DeFi). Special regulations that are designed comprehensively and based on the principles of modern justice can be the foundation for clearer criminal accountability, prevent impunity for perpetrators, and provide certainty and fair legal protection for all parties, including victims of crimes in the crypto world.

In designing special criminal regulations that can answer the challenges of the crypto world, a significant first step is to establish a clear and operational legal definition of the various digital entities that are part of this ecosystem. Digital assets, smart contracts, decentralized finance (DeFi), and crypto wallets are technical terms that have different legal dimensions from entities in the conventional financial system. Without a clear definition, law enforcers will have difficulty in identifying legal objects, evidence, and scope of actions that can be qualified as criminal acts. For example, digital assets need to be defined not only as commodities or means of exchange, but also as investment objects and instruments that have a certain economic value, both speculative and functional. Likewise, smart contracts must be understood as automatic codes that regulate legal relations between parties without intermediaries, so that separate assessments are needed regarding their validity, responsibility, and legal effects in a criminal context.

Furthermore, regulations must explicitly determine who can be criminally responsible in a decentralized system. This is the most challenging aspect because blockchain and DeFi systems do not have a central entity or single authority that can be held accountable as in the traditional banking system. In many cases, the perpetrators who design and launch smart

contracts no longer have control over the application once launched on-chain. Therefore, the criminal law approach must be adjusted to allow for the application of criminal liability to developers, operators, digital wallet service providers, as well as individuals or entities that benefit from criminal acts on the platform. The approach of collective criminal liability, strict liability, or even a form of corporate criminal liability can be considered, depending on the role and level of involvement of each party in the crime.

Apart from determining who can be held responsible, regulations must also formulate new criminal acts that cover forms of digital crime that are unique to the crypto ecosystem. For example, rug pull as a form of fraud where a crypto project developer suddenly withdraws investor funds and disappears, should be formulated as a separate criminal act because it is not entirely relevant if it is only subject to Article 378 of the Criminal Code. Likewise, blockchain-based phishing which is carried out by directing victims to access fake wallets, as well as digital wallet hacking without touching physical infrastructure, all require the formulation of crimes that not only reflect malicious intent (mens rea) but also take into account technical characteristics of the tools and methods used. Without a specific crime formulation, law enforcement officers will continue to face obstacles in proving criminal elements imposed by the conventional legal framework.

Equally important, regulations must strictly regulate criminal provisions related to illegal transactions, crypto asset market manipulation, and blockchain-based money laundering. Many criminals use digital asset trading mechanisms to carry out insider trading, spoofing, or price manipulation that harms other investors, and this practice does not yet have a specific criminal law basis in Indonesia. On the other hand, due to the anonymous and borderless nature of blockchain, crypto assets are very vulnerable to being used as a means of cross-border money laundering that is difficult to track. Therefore, it is necessary to design provisions that not only stipulate prohibitions, but also regulate standards for verification, reporting, and cross-jurisdictional cooperation, including with foreign authorities and technology providers.

The approach to criminal liability in a decentralized ecosystem must be adapted to the unique nature of blockchain technology which does not have a central authority. In this context, one relevant approach is the collective criminal liability model, whereby several parties involved in the development, distribution, or operation of a system that supports criminal activity, such as a DeFi platform or a problematic smart contract protocol, can be held jointly responsible. This approach emphasizes the principle that digital crimes are often the result of collaboration between various parties, whether from a technical, financial, or ideological

perspective. In addition, a technology-independent approach can also be applied, namely focusing responsibility not solely on the system or algorithm, but on the role and contribution of humans in creating the conditions that allow the crime to occur. This is important so that the law does not get caught up in overly technical proof, but rather sees human involvement as the main factor in the element of guilt (mens rea).

In a decentralized system, actors such as smart contract developers and DeFi platform operators occupy strategic positions that allow them to influence the security and integrity of the system. Therefore, it is important to establish the limits of criminal liability for them. Developers who intentionally create smart contracts with exploitative loopholes, or even build rug pull mechanisms hidden in the code, can be qualified as the main perpetrators of fraud or embezzlement of digital assets. Meanwhile, DeFi operators, although they do not always control transactions directly, can still be held accountable if they are proven to be negligent in implementing identity verification mechanisms (Know Your Customer), or if they facilitate money laundering without a due diligence process. In this case, an adaptive criminal approach needs to be applied, considering the position, role, and awareness of the risks posed by each party in the decentralized system structure.

Two models that can be used as a basis for analysis to develop criminal liability in crypto are strict liability and vicarious liability. Strict liability allows the imposition of criminal sanctions without the need to prove malicious intent, simply based on the act and its legal consequences. This model is suitable for cases of regulatory violations or systemic negligence that have a wide impact, such as allowing money laundering activities through platforms that do not have a reporting system. Meanwhile, vicarious liability allows for accountability for entities or individuals for the actions of others in one organizational structure, such as the owner or manager of a crypto project operated by a development team. This model is useful in the context of the DeFi ecosystem whose operations are spread out and do not always involve a single actor. Selective adoption of these two models in the new criminal law framework will provide law enforcement with the flexibility to reach crypto criminals who hide behind the anonymity and complexity of technology.

To address the complexity of crimes in the crypto ecosystem, a comprehensive criminal law regulatory framework must start by expanding the scope of Indonesian criminal law jurisdiction to crimes committed across countries or in digital spaces without territorial boundaries. In the context of blockchain technology which is global and without a center, traditional jurisdiction based on territory is inadequate. Therefore, an extraterritorial jurisdiction approach is needed, where Indonesian criminal law can be applied to perpetrators

of crypto crimes that have a direct impact on Indonesian citizens or the national financial system, even though the perpetrators are abroad. To support this, Indonesia must actively strengthen international cooperation, through bilateral agreements, participation in cross-border organizations, and integration with international legal protocols related to cybercrime and money laundering based on digital assets.

In addition to the jurisdictional aspect, the establishment of a special institution or unit that specifically handles crypto crimes is also a major urgency. Crimes in the crypto realm require technical expertise, digital forensics, and a deep understanding of blockchain and DeFi technology—things that conventional law enforcement officers do not yet fully possess. Therefore, it is necessary to form an integrated law enforcement unit consisting of criminal investigators, technology analysts, digital financial experts, and cyber intelligence who work collaboratively across sectors. This unit can be under the coordination of the Attorney General's Office or the National Police but has close connections with financial supervisory institutions such as PPATK, OJK, and BI. The establishment of this special unit will also increase efficiency in tracking digital assets hidden through complex transactions or sent to anonymous wallets abroad.

Furthermore, criminal regulations against crypto crimes must be integrated with the financial and digital technology regulatory system so that there is no overlap or gap in supervision. This integration includes harmonization between criminal regulations governing sanctions and crimes, with administrative and compliance provisions in the digital financial sector, including crypto asset trading, digital wallets, and DeFi platforms. For example, criminal sanctions must apply to perpetrators who violate compliance rules such as failing to report suspicious transactions or not carrying out the user identity verification process. This integration also allows for the strengthening of data-based law enforcement, where transaction information from digital asset service providers can be used as valid evidence in criminal courts.

A clear mapping of roles and authorities is needed between the institutions involved, namely BAPPEBTI, Bank Indonesia (BI), Financial Services Authority (OJK), Financial Transaction Reports and Analysis Center (PPATK), and the police. BAPPEBTI has a central role in regulating and supervising the trading of crypto assets as commodities but does not yet have criminal authority. OJK and BI, although not yet directly supervising crypto assets, must begin designing a monitoring mechanism for digital assets that are stable (such as stablecoins) and used as illegal exchange tools. PPATK plays an important role in tracking suspicious financial transactions but must be supported by broader and faster data access from crypto asset

business actors. Meanwhile, the police must be given special training and a technological support system to conduct investigations effectively. Collaboration between these institutions must be formally stated in new regulations so that there is no conflict of authority, and the entire law enforcement process can run in an integrated, responsive, and adaptive manner to technological developments.

4. CONCLUSION

This study shows that the criminal law system in Indonesia is currently unable to effectively accommodate the development of crimes in the anonymous, cross-border, and decentralized crypto ecosystem. Existing positive legal provisions, such as Article 378 of the Criminal Code, Article 28 paragraph (1) of the ITE Law, as well as provisions in the TPPU Law and the Banking Law, still depart from the conventional legal paradigm that relies on clear legal subjects, limited jurisdiction, and visible physical evidence. This makes it difficult to prosecute many crypto criminals and many victims do not receive adequate legal protection or recovery. Legal vacuums and unclear regulations not only weaken the effectiveness of law enforcement, but also create legal uncertainty that risks harming public trust in the national legal and financial systems. Therefore, an adaptive, technology-based criminal law approach is needed that can reach new forms of crime in the digital realm.

In response to these problems, it is important for policy makers to immediately design special criminal regulations that comprehensively regulate crypto-based crimes, including regulations regarding the legal definition of digital assets, smart contracts, and DeFi systems; formulation of new criminal offenses such as rug pull, wallet hacking, and blockchain-based money laundering; as well as provisions regarding legal subjects in a decentralized system. In addition, it is necessary to form a special unit to handle crypto crimes with cross-field competence—law, finance, and technology. The new regulations must also be harmoniously integrated with the financial regulation system and information technology supervision, while expanding the jurisdiction of Indonesian criminal law extraterritorially to reach perpetrators who operate from abroad but have an impact on the domestic system. With these steps, it is hoped that the Indonesian criminal law system will be able to provide fair and effective legal protection in the digital era.

REFERENCES

Arwani, A. &. (2024). Eksplorasi Peran Teknologi Blockchain Dalam Meningkatkan Transparansi DanAkuntabilitas Dalam Keuangan Islam: Tinjauan Sistematis. Jurnal Ekonomi Bisnis Dan Manajemen, 2(2), 23-37. https://doi.org/10.59024/jise.v2i2.653

Astrawan, I. K. (2021). Perlindungan Hukum bagi Pemegang Kartu E-Money Sebagai Alat Pembayaran dalam Transaksi Non Tunai. Jurnal Interpretasi Hukum, 2(1), 132. https://doi.org/10.22225/juinhum.2.2.3442.366-371

Buckley, R. P. (2020). Cryptoassets: Legal, regulatory, and monetary perspectives. New York: Oxford University Press.

Budiman, M. A. (2020). Regulation of cryptocurrency in Indonesia: a comparative study with Singapore and Malaysia. Journal of Indonesian Economy and Business, 35(2), 155-172.

Chong, S. e. (2022). Comparative analysis of cryptocurrency regulation in Southeast Asia. Singapore Journal of Legal Studies, 1(1), 1-25.

Darmawan, O. &. (2020). Apakah bitcoin standar uang masa depan?: mengungkap sejarah dan hakikat uang, serta sistem desentralisasi bitcoin. Yogyakarta: Media Pressindo.

Herlambang, R. (2020). Crypto assets and Indonesian legal system. Procedia Computer Science, 17(6), 145-154.

Ilyasa, R. M. (2019). Legalitas Bitcoin Dalam Transaksi Bisnis Di Indonesia. UKM Lex Scientia, 2(2), 112. https://doi.org/10.15294/lesrev.v3i2.35394

Lestari, H. T. (2024). Potensi, Tantangan, Dan Implementasi Blockchainuntuk Pengembangan Aplikasi Dalam Era Digital Modern. Journal Warunayama, 5(3), 1-23.

Martinelli, I. M. (2024). egalitas Dan Efektivitas Penggunaan Teknologi Blockchain Terhadap Smart Contract Pada Perjanjian Bisnis Di Masa Depan. Unes Law Review, 6(4), 10761-10776.

Noorsanti, R. C. (2018). Blockchain - Teknologi Mata Uang Kripto (Crypto Currency). Prosiding SENDI_U, 12-13.

Purwanto, D. (2021). Cryptocurrencies fraud in Indonesia: a legal perspective. Jurnal Hukum, 28(2), 231-246.

Rahayu, A. (2021). Consumer protection in the digital economy: the case of Indonesia. Journal of Consumer Policy, 44(2), 151-170.

Rahmanto, D. &. (2020). Penerapan Peraturan Perundang-Undangan yang Melarang Penggunaan Produk Crypto sebagai Alat Pembayaran Maupun Subyek Komoditas yang Bisa diperdagangkan Melalui Bursa Berjangka di Indonesia. Jurnal Hukum Adil, 11(2), 33. https://doi.org/10.33476/ajl.v11i2.1648

Razzaq, R. G. (2018). Legalitas Mata Uang Virtual dalam Perspektif Hukum Indonesia. Jurnal Lontar Merah, 1(2), 344.

Rinaldi, D. A. (2016). Bitcoin sebagai Alat Pembayaran Online dalam Perdagangan Internasional. Perspektif Hukum, 16(1), 445.

Rohman, M. N. (2021). Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia. Jurnal Supremasi, 11(2), 344. https://doi.org/10.35457/supremasi.v11i2.1284

Sajidin, S. (2021). Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran di Indonesia. Arena Hukum, 14(2), 55. https://doi.org/10.21776/ub.arenahukum.2021.01402.3

Tauda, R. (2023). Cryptocurrencies: Highlighting the approach, regulations, and protection in Indonesia and the European Union. BESTUUR, 11(1), 1-12. https://doi.org/10.20961/bestuur.v11i1.67125

Wijaya, D. A. (2016). Mengenal Bitcoin dan Cryptocurrency. Medan: Puspantara.