Indonesian Journal of Criminal Law Studies
ISSN 2548-1568 (Print) 2548-1576 (Online)
Vol. 10 Issue 1 (2025) 297-340
The title has been indexed by **SCOPUS**, **SINTA**
DOI: https://doi.org/10.15294/ijcls.v10i1.22557
Online since: June 13, 2025

Indonesian Journal of CRIMINAL LAW STUDIES

A peer-reviewed journal published by **Faculty of Law Universitas Negeri Semarang, Indonesia**.
Online at https://journal.unnes.ac.id/journals/ijcls/index

Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law

David Hardiago[a]✉, Rani Fadhila Syafrinaldi[a], Syafrinaldi[a], M. Musa[a], Kim Hyeonsoo[b]

[a] Faculty of Law Universitas Islam Riau, Riau, Indonesia
[b] School of Law, INHA University Seoul, South Korea

✉Corresponding Email: davidhardiago23@law.uir.ac.id

Abstract

The advancement of science and technology continues to accelerate. Internet and its supporting technology became the backbone for many activities. This kind of advancement goes beyond territorial boundaries and human's intelligence. This phenomenon triggers a new crime model. One of them is a crime related to the existence of Cryptocurrency such as money laundering, terrorism financing, and other forms of crime. This is understood given that Cryptocurrency give rise to large number of crimes as well as the emergence of a new modus operandi in several criminal acts. This is further supported by the lack of current Indonesian regulations that do not specifically accommodate the Cryptocurrency mechanism. The main issues raised in this study are related to how crimes and new modus operandi are caused by the Cryptocurrency mechanism against Indonesian criminal law, as well as how the mechanism of crime prevention and handling caused by the Cryptocurrency mechanism through the means of

penal policy, covering targeted legislative amendments, specialised investigative units, prosecutorial guidelines, and asset-seizure procedures—to prevent and combat such crimes. This article uses normative method to answer the problem through comparative approach, case approach, literary approach and statutory approach. Initial hypotheses proposed to address these problems are: First, Cryptocurrency as a financial transaction mechanism that relies on the computational system with anonymous transactions opens a great opportunity for crime in the mechanism of the transaction. Second, the establishment of new rules in order prevent and combat crime and the modus operandi caused by the Cryptocurrency mechanism through the mechanism of penal policy are essential.

Keywords
Criminal Act; Cryptocurrency; Penal Policy.

HOW TO CITE:
Chicago Manual of Style Footnote:
[1] David Hardiago, Rani Fadhila Syafrinaldi, Syafrinaldi, M. Musa, and Kim Hyeonsoo, "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law", *Indonesian Journal of Criminal Law Studies 10*, no 1 (2025): 297-340, https://doi.org/10.15294/ijcls.v10i1.22557.

Chicago Manual of Style for Reference:
Hardiago, David, Rani Fadhila Syafrinaldi, Syafrinaldi, M. Musa, and Kim Hyeonsoo, "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law", *Indonesian Journal of Criminal Law Studies 10*, no 1 (2025): 297-340, https://doi.org/10.15294/ijcls.v10i1.22557.

Introduction

The industry, spanning various sectors and fields, both in production and services, has undergone a series of developments commonly referred to as the "Industrial Revolution".[1] Mechanisation (Industry 1.0), mass electrification (2.0), computerised automation (3.0), and today's cyber-physical convergence (Industry 4.0).[2] Examining cryptocurrency within this fourth stage is urgent for three, mutually reinforcing reasons: Juridically, Indonesia's existing criminal-law corpus (KUHP, UU ITE, and anti-money-laundering statutes) was drafted for centrally cleared payment systems. Cryptocurrency's borderless and pseudonymous character reveals a doctrinal void on seizure, forfeiture, and rules of evidence that need to be addressed by the legislature to maintain lex certa and legal certainty. Philosophically, the Constitution binds the state to protect the economic welfare of people and provide justice. Allowing value networks outside of regulation that facilitate fraud, ransomware, and tax evasion is a disregard for those founding principles; an appropriate regulatory regime therefore becomes a moral obligation to balance innovation with the common good. Sociologically, currently, almost 30 million Indonesians use crypto exchanges, and token and online gambling scams amount to losses that have exceeded IDR 3 trillion for the year 2024, furthermore, the country has suffered losses in amount of IDR 1.3 trillion due to illicit crypto activity.[3]

Public adoption outpaces institutional capacity, creating real victims and eroding trust in digital-economy programmes unless effective preventive and enforcement mechanisms are put in place. Together, these juridical, philosophical, and sociological considerations

---

1 Revolution Refers To A Transformation In Social Structures, Culture, And Societal Habits That Impact The Fundamental Aspects Of Community Life In A Brief Period. Industry Is An Economic Activity That Processes Raw Materials Into High-Quality Goods. See Nova Jayanti Harahap, "Mahasiswa Dan Revolusi Industri 4.0," Ecobisma (Jurnal Ekonomi, Bisnis Dan Manajemen) 6, no. 1 (2019): 70–78, https://doi.org/10.36987/ecobi.v6i1.38.

2 Yongxin Liao et al., "The Impact of the Fourth Industrial Revolution: A Cross-Country/Region Comparison," *Production* 28, no. January (2018), https://doi.org/10.1590/0103-6513.20180061.

3 Wilda Hayatun Nufus, "Kejagung Temukan Aliran Kripto Ilegal Bikin Negara Rugi 1,3 Triliun," detiknews, February 6, 2025. https://news.detik.com/berita/d-7766518/kejagung-temukan-aliran-kripto-ilegal-bikin-negara-rugi-rp-1-3-triliun

demonstrate why Indonesia must urgently reassess its criminal-law tools in the face of Industry 4.0's decentralised financial architectures.The industry 4.0, whichcan be simply described as a "digital revolution", where the proliferation of the Internet of Things (IoT) and interconnectivity across various aspects, including industrial business contexts, leads to the blurring of boundaries between the physical and digital dimensions giving rise to decentralised payment systems such as cryptocurrency.[4]

Over the past decade, an emerging literature has examined cryptocurrency from economic, technical, and regulatory perspectives. Narayanan et al. (2016)[5] illustrated the cryptographic theories that form the basis of Bitcoin and demonstrated how its peer-to-peer nature circumvents traditional monetary regulation. Foley, Karlsen and Putniņš (2019)[6] estimated that about 46 % of Bitcoin transactions relate to illegitimate activity, emphasizing the criminal allure of the technology. From a Southeast-Asian perspective, empirical research written by Nelson, Prosperiani, Ramadhan, and Andini (2024)[7] examines the challenging process of tracing, confiscating, and recovering cryptocurrencies used in money-laundering operations by Indonesian law enforcement. By means of literature review and interviews, they demonstrate that the multi-layered security of blockchain has compelled police investigators and prosecutors to utilize both penal tools (like official seizure orders) and non-penal measures (like informal collaboration with foreign FIUs and Interpol) to chase crypto proceeds disseminated across Indonesia's jurisdiction. Their Indra Kesuma case study identifies the manner in which legal uncertainty relating to custody of assets generated procedural

---

4 Marcelo Negri Soares and Marcos Eduardo Kauffman, "Industry 4.0: Horizontal Integration and Intellectual Property Law Strategies In England," *Revista Opinião Jurídica (Fortaleza)* 16, orang. 23 (2018): 268, https://doi.org/10.12662/2447-6641oj.v16i23.p268-289.2018.

5 Arvind' "Bonneau, Joseph" "Edward, Felten" "Miller, Andrew" "Goldfeder, Steven" 'Narayanan, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, 1st ed., vol. 1 (New Jersey: Princeton University Press, 2016).

6 Sean Foley et al., "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?,"http://www.emcdda.europa.eu/attachements.cfm/att_194336_EN_TD3112366ENC.pdf.

7 Mutiara, Febby' "Prosperiani, Maria, Dianita" "Ramadhan, Choky, Risda" "Andini, Priska, Putri" 'Nelson, "Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia ," *Journal of Indonesian Legal Studies* 9, no. 1 (May 8, 2024): 89–130.

objections that ultimately prevented recovery. To address these shortcomings, they suggest a package of tailored tools, orders of seizure, orders of confiscation, and pre-confiscation sale that would help further improve Indonesia's ability to manage and dispose of seized crypto assets effectively.[8]

Recalling these working observations, Sari and Rahim (2024)[9] also talk about the evidence aspect of crypto assets in criminal prosecutions. They show how quickly fluctuating asset values and how easily tokens are transferable or can be anonymized create demands for timely, legally sustainable control to satisfy the exclusionary rule and preserve evidentiary integrity from investigation through trial and enforcement. Their work unveils a shocking lack of any binding procedural framework for the acceptance and preservation of crypto assets as genuine evidence, resulting in divergent practices and necessitating a standard national procedure for handling digital-asset evidence.[10] Finally, an article by Fathi, Al-Shammar, and Mohamed (2025) published in the Journal of Money Laundering Control presents a comparative perspective from Saudi Arabia's effort to curb cryptocurrency-enabled financial crimes. Using content analysis of legal reform, case studies, and doctrinal sources, they conclude that despite recent regulatory reforms, the Saudi system continues to be beset by inadequate public awareness, limited law-enforcement powers, and a lack of international cooperation to monitor and deter crime in decentralized networks. Their findings reaffirm the worldwide position of these problems and bolster the thesis that Indonesia must not only refine its domestic legislations but also strengthen cross-border collaboration and capacity building so as to effectively counter crypto-facilitated crime in Industry 4.0.[11]

Collectively, these writings expose two imminent gaps. First,

---

8 Ibid.

9 Desty Puspita Sari et al., "Handling Of Crypto Assets As Evidence In Criminal Cases," *The Prosecutor Law Review* 03, no. 1 (2025), https://bappebti.go.id/pojok_media/detail/11410,.

10 Ibid.

11 M' "Al-Shammar, bin Saud M" "Khalifa, Mohamed" 'Fathi, "Cryptocurrency and Criminal Liability: Investigating Legal Challenges in Addressing Financial Crimes in Decentralized Systems," Journal of Money Laundering Control, 28, no. 3 (May 14, 2025): 504–17, https://doi.org/https://doi.org/10.1108/JMLC-07-2024-0110.

regulatory lag: while Indonesia's Commodity Futures Supervisory Agency (BAPPEBTI) acknowledges crypto as a commodity that can be traded, the KUHP, the Anti-Money-Laundering Act, and the ITE Law have not yet incorporated specific provisions for seizing or forfeiting digital assets. Second, institutional readiness: the police, PPATK, and the courts still rely on legacy investigative tools ill-suited to pseudonymous ledgers. This article therefore offers three novel contributions. First, a doctrinal synthesis that organized interpretation of fragmented statutory provision applicable to crypto-related offences and tests their adequacy against real-world typologies (ransomware, investment fraud, darknet markets). Second, an institutional capacity audit, drawing on PPATK analysis, data not yet covered in prior literature, to measure Indonesia's operational ability to trace, freeze, and forfeit crypto assets. Third, a policy blueprint proposing an integrated amendment package, substantive, procedural, and organisational, that aligns Indonesia's criminal-law apparatus with Industry 4.0 realities while preserving innovation incentives.

As part of the continuous development of technology and information, Industry 4.0 possesses distinct characteristics that mark the beginning of this new era. Fundamentally, Industry 4.0 is distinguished by increased mobility, enhanced access to information, and the growing number of smart devices that enable the integration of labor, machinery, human resources, and products into a unified data network.[12]

As with previous industrial revolutions (from the First to the Third Industrial Revolution), the ongoing Fourth Industrial Revolution has introduced significant changes across various aspects of society. This study specifically examines the electronic transaction (e-commerce) sector and its legal implications within Indonesia's criminal law framework. In contemporary practice, the evolution of new trade and financial systems through electronic media (e-commerce) has led to the integration of cryptocurrency as a transaction method. This digital currency model emphasizes decentralization, which significantly alters traditional transaction mechanisms. Unlike conventional financial transactions that

---

[12] Lalu Adi Adha, "Digitalisasi Industri Dan Pengaruhnya Terhadap Ketenagakerjaan Dan Hubungan Kerja Di Indonesia," *Journal Kompilasi Hukum* 5, no. 2 (2020): 267–98, https://doi.org/10.29303/jkh.v5i2.49.

rely on third-party institutions (such as banks) to record and authenticate transactions, blockchain technology enables peer-to-peer transactions, allowing individuals to manage their transactions independently.[13] Blockchain technology was developed as a response to the lack of trust in conventional databases managed by third parties. As such, there was a need for a new technology to address this mistrust.[14] Through the use of cryptocurrency and blockchain technology as a method of transaction, the tracking of transaction flows and the amount of transactions can be carried out confidentially between parties and without detection by any third party. Moreover, cryptocurrency as a financial transaction mechanism also offers the ability to conduct transactions anonymously, both for the party sending the digital currency and for the party receiving the transaction. This anonymity feature is one of the key factors that distinguish cryptocurrency from traditional financial systems and poses challenges for regulatory bodies seeking to ensure transparency and prevent financial crimes.[15]

In most jurisdictions, the use of cryptocurrency as a means of transaction and payment, commonly known as cryptocurrency transactions, is classified as a legal activity. This is due to the fact that regulations in those countries permit transactions involving cryptocurrency.[16] However, despite the fact that some countries have regulated transactions involving cryptocurrency as a legal activity, this does not apply universally across all nations. Some countries, including Indonesia, still treat transactions using cryptocurrency as ambiguous, leading to ongoing debates about whether such transactions are legal. The debate surrounding the legality of cryptocurrency transactions in Indonesia is influenced by the lack of a clear legal framework that defines

---

13 Trinita Imelda Bandaso, Fransiskus Randa, and Frischa Faradilla Arwinda Mongan, "Blockchain Technology: Bagaimana Menghadapinya? – Dalam Perspektif Akuntansi," *Accounting Profession Journal* 4, no. 2 (2022): 97–115, https://doi.org/10.35593/apaji.v4i2.55.

14 Neil Tiwari, "The Commodification of Cryptocurrency," *Michigan Law Review* 117, no. 3 (2018): 611–34, https://doi.org/10.36644/mlr.117.3.commodification.

15 Syahrul Sajidin, "Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran Di Indonesia," *Arena Hukum* 14, no. 2 (2021): 245–67, https://doi.org/10.21776/ub.arenahukum.2021.01402.3.

16 Witold Srokosz and Tomasz Kopyciaski, "Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability 1," *Journal of Teaching and Education* 04, no. 02 (2015): 619–27, http://www.loc.gov/law/help/bitcoin-.

the validity of cryptocurrency transactions. This lack of legal clarity remains a key factor in the ongoing uncertainty over the legal status of cryptocurrency transactions within the country.[17]

The legal uncertainty surrounding cryptocurrency transactions in Indonesia is largely influenced by the absence of a clear legal framework governing the legitimacy of cryptocurrency transactions. This ambiguity is further exacerbated by a conflict between two primary regulations: first, Article 8(1)(d) of Bank Indonesia Regulation No. 19/12/PBI/2017 on the Implementation of Financial Technology (referred to as BI Regulation 2017), which explicitly states that all transactions in the financial technology sector conducted in Indonesia must use the Rupiah as the currency of exchange, and prohibits the use of virtual currencies as a medium of exchange or payment (Article 8(2) of BI Regulation 2017). On the other hand, the Commodity Futures Trading Regulatory Agency (BAPPEBTI) issued Regulation No. 3 of 2019 regarding Commodities Eligible for Futures Contracts, Sharia Derivative Contracts, and/or Other Derivative Contracts Traded on Futures Exchanges (referred to as BAPPEBTI Regulation No. 3 of 2019), which states in Article 1(f) that crypto assets can be used as commodities eligible for trading. Indirectly, this regulation opens the door for cryptocurrency to be used in commercial transactions as an asset. Thus, the regulatory conflict between these two legal provisions contributes to the ongoing debate and uncertainty surrounding the legal status of cryptocurrency transactions in Indonesia.

The conflict between the two regulations concerning the validity of cryptocurrency transactions in Indonesia ultimately leads to the absence of a clear legal framework, especially at the legislative level, that explicitly defines the legal status of cryptocurrency in Indonesia. Given the transactional model of cryptocurrency, which carries a high risk of misuse due to the blockchain technology and the anonymous transaction system, this creates significant opportunities for it to be used as a vehicle for criminal activities. Such misuse can give rise to criminogenic factors in the realm of digital financial transactions, particularly in cyber laundering.

---

17 Ibid.

For instance, an article published on the media platform Kontan.co.idnotes that the FBI had gathered at least 130 cases in 2018 related to crimes involving cryptocurrency, with money laundering and tax evasion being the two most predominant offenses among the total cases.[18]

Crimes facilitated by cryptocurrency mechanisms are still relatively unfamiliar compared to other economic crimes such as corruption, money laundering, tax evasion, banking crimes, and others currently occurring in Indonesia. However, when compared to other countries, crimes resulting from cryptocurrency transactions have already been classified as a fairly familiar model of criminal activity. For instance, this can be illustrated by the case handled by the U.S. Department of Justice involving Ross William Ulbricht in 2015. In this case, Ulbricht, the owner of Silk Road, using the alias Dread Pirate Roberts, conducted illegal transactions involving the sale of various illicit drugs, with payments processed through Bitcoin as part of the cryptocurrency mechanism. The profits from these illegal transactions amounted to USD 1 billion.[19]

Another example related to crimes arising from cryptocurrency mechanisms can be seen in cases currently being handled by the FBI, which involve human trafficking, money laundering, terrorism financing, and illegal trade (such as illegal weapons, drugs, etc.), where all these crimes involve transactions facilitated by cryptocurrency technology. Given the scope of these cases, further analysis is necessary to understand the criminogenic factors resulting from the use of cryptocurrency as a transaction mechanism. Additionally, it is crucial to project and develop effective prevention and regulation mechanisms for cryptocurrency within Indonesia's criminal law framework. Such measures are essential for ensuring that cryptocurrency-related crimes can be effectively managed and mitigated in the future.

---

18 Muttaqim Muttaqim and Desi Apriliani, "Analysis of The Probability of Money Laundering Crimes toward the Development of Crypto-Currency Regulations in Indonesia," *IJCLS (Indonesian Journal of Criminal Law Studies)* 4, no. 1 (2019): 29–40, https://doi.org/10.15294/ijcls.v4i1.18714.

19 Anthony Minnaar, "Online 'Underground' Marketplace for Illicit Drugs : The Prototype Case of the DarkWeb Website 'Silk Road,'" *Acta Criminologia : Southern African Journal of Criminology* 30, no. 1 (2017): 23–47, https://www.researchgate.net/publication/333646270.

Method

Doctrinal research was chosen for its of its ability to analyze and interpret legal rules within depth reasoning, basing each step firmly in established legal literature.[20] As explained by McConville and Wing, legal research is divided into "doctrinal and non-doctrinal" research.

A doctrinal method is appropriate for this study because its questions are strictly legal: it interprets Indonesia's existing criminal-law provisions (KUHP, UU TPPU, UU ITE, Bappebti rules) to detect doctrinal gaps in handling crypto-asset offences; benchmarks those findings against foreign frameworks (e.g., MiCA, U.S. DAAML Act) to identify best practices; and ultimately formulates precise statutory amendments, prosecutorial guidelines, and asset-seizure procedures—deliverables that rely on authoritative legal texts rather than empirical field data.[21]

In order to bring together materials, we examined the Indonesian Ministry of Law and Human Rights website and online repository of the Supreme Court for all relevant legislation, regulations, and court judgments printed and online. Treatises and scholarly journal articles were then accessed via JSTOR, other relevant journals and the Indonesian university repositories, legal dictionaries and encyclopedias providing necessary terminological accuracy. With a combination of keyword search queries, such as with "cryptocurrency," "blockchain," and "criminal," we ensured that root and advanced sources were covered.

Additionally, as doctrinal legal research, the data sought in this study is secondary data.[22] This secondary data will consist of legal materials, which

---

20 Salim Ibrahim Ali et al., "Legal Research of Doctrinal and Non-Doctrinal," *International Journal of Trend in Research and Development* 4, no. 1 (May 2017): 2394–9333, www.ijtrd.com.

21 Maria S.W Suwardjono, *Metodelogi Penelitian Ilmu Hukum* (Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2014).

22 Maria S.W Suwardjono, *Bahan Kuliah: Metodelogi Penelitian Hukum* (Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2014).

include primary legal materials,[23] secondary legal materials,[24] and tertiary legal materials. The research will also be supported by several approaches, those include statutory approach, conceptual approach, case approach, dan comparative approach.[25] Once assembled, these legal materials underwent a qualitative content analysis in which statutory provisions and judicial opinions were coded inductively according to emerging themes—for example, "transaction anonymity," "predicate-offense ambiguity," and "regulatory conflict".

Result and Discussion

A. Legal Challenges of Cryptocurrency-Related Crimes: Urgency for Reform in Indonesian Criminal Law

This sub-chapter provides a critical review of the relationship between cryptocurrency technology and law enforcement in Indonesia. There are already increasing calls for legally responsive regulation to keep pace with the speed at which crypto-based financial activities are disrupting what law defines a crime and what authority is available to the state to maintain some regulatory control. Within this sub-chapter, we shall examine three main issues: the basic characteristics of cryptocurrency and sources of legal ambiguity; the types of criminal transactions that cryptocurrency technology allows (especially those assist the undermining of economic integrity); and the gaps in Indonesia's existing legal and institutional arrangements obstructing their ability to detect, deter, and prosecute those crimes.

This sub-chapter also provides a critical examination of the strained relationship between cryptocurrency technology and Indonesia's law enforcement and why drastic action can no longer waits. Since it became

---

23 Primary Legal Sources Include Legally Binding Legal Materials, Consisting Of: A. Fundamental Norms Or Basic Rules, Such As The Preamble Of The 1945 Constitution, B. Basic Regulations, C. Legislation, D. Uncodified Legal Materials, Such As Customary Law, E. Jurisprudence, F. Treaties, G. Legal Materials From The Colonial Era That Are Still Valid, Such As The Criminal Code (Kuhp).See Soerjono Soekamto, Penelitian Hukum Normatif: Suatu Tinjauan Singkat (Jakarta: Rajawali Press, 2015).

24 Ibid.

25 Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2005).

established in Indonesia five years ago, crypto-aided money-laundering and tax-evasion schemes have rapidly expanded worldwide. FBI reports have monitored over 130 individual cryptocurrency-linked investigations alone in 2018[26] and Indonesia's Bitcoin daily trade volume has reached over IDR 4 billion[27], creating an environment susceptible to abuse. Yet our legal framework still lags behind: ambiguous definitions leave "predicate offenses" open to interpretation, conflicting regulations pit Bank Indonesia against BAPPEBTI, and no institution is specifically empowered to pursue blockchain crimes. Within this sub-chapter, we examine three urgent fault lines that demand immediate reform: the core characteristics of cryptocurrency that enable concealed, pseudonymous transaction flows; the novel criminal schemel, ranging from cyber-laundering to invisible-wallet tax evasion that exploit these features to to undermine economic stability; and the gaping holes in Indonesia's current legal and institutional framework that delay timely detection, deterrence, and prosecution of these crimes.

A.1 Cryptocurrency General Overview

The definition of cryptocurrency, as found in various literatures, does not exhibit uniformity. Among the various opinions, one definition states:[28]

> *"Cryptocurrency is succinctly defined as a unit of value stored in an electronic medium. Cryptocurrency is not created by a government or monetary authority, but by a group of individuals or legal entities aiming to be used for the exchange of goods multilateral or between group members. With an 'open' or 'closed' digital currency scheme, it depends on whether or not it can be converted into legal currency."*

---

26 Lily' "Massa, Annie" 'Katz, "FBI Has 130 Cryptocurrency-Related Investigations, Agent Says Trafficking, Drugs, Kidnapping, Ransomware Cases under Review Agency Has Noticed an Increase in Crypto-Related Crimes," Bloomberg, June 28, 2018.

27 Hendro' 'Situmorang, "Indonesia's Crypto Trading Soars 335% to Reach $40 Billion in 2024," Jakartaglobe, January 25, 2025.

28 Muttaqim And Apriliani, "Analysis Of The Probability Of Money Laundering Crimes Toward The Development Of Crypto-Currency Regulations In Indonesia."

Another definition of cryptocurrency is understood as a complex digital-software mechanism consisting of a payment system, where transactions can be made through cryptocurrency tokens as a unit of value exchange within the blockchain system. Simultaneously, the data transfer protocols, transaction verification codes, and the public database of all transactions ever made are managed by all participants and updated on all computers after each transaction in the system is executed.[29] Therefore, cryptocurrency is not money in the classical sense, but it has a market value determined by the demand and supply of account units and internal costs equivalent to the price of services or goods obtained within the exchange chain.[30] The understanding of cryptocurrency transaction patterns can be referenced from the perspective of Martin Vejacka, as follows:[31]

> *"The basic principle of cryptocurrency is that no individual (or organization) can accelerate or significantly misuse the production of a specific currency. Typically, only a certain amount of cryptocurrency is collectively produced by the entire cryptocurrency system. The production rate is determined by a predefined value, which is made publicly known. Cryptocurrency allows for the transfer of cryptocurrency units, commonly referred to as coins, between the applications of one subject and another through a peer-to-peer computer network, with almost no transaction costs."*

In the context of finance and digital transactions, cryptocurrency is considered a relatively new transaction model compared to other digital financial technologies. Referring to its historical context, cryptocurrency, as a virtual currency utilizing a payment system that is untraceable due to the use of cryptography as

---

29 Imelda Bandaso, Randa, And Arwinda Mongan, "Blockchain Technology: Bagaimana Menghadapinya? – Dalam Perspektif Akuntansi."

30 Valeriia Dyntu, "Cryptocurrency As A Means Of Money Laundering," Baltic Journal Of Economic Studies 5, No. 1 (2018): 267–71, Https://Doi.Org/Https://Doi.Org/10.30525/2256-0742/2018-4-5-75-81.

31 Martin Vejačka, "Basic Aspects Of Cryptocurrencies," N.D., 75–83.

part of blockchain technology, has been known for the past ten years.[32] Specifically, cryptocurrency refers to a system that uses cryptography to enable secure transfer and exchange of digital tokens in a distributed and decentralized manner, first introduced in 2009. The tokens involved in cryptocurrency transactions can be traded according to market prices and later exchanged for traditional currencies (currencies of specific countries).[33]

Cryptocurrency, with the first virtual currency known as Bitcoin, began being traded in January 2009. Bitcoin remains the most popular and prominent cryptocurrency to date. The technical design for Bitcoin was introduced in 2008, published by an unknown individual or group under the pseudonym Satoshi Nakamoto.[34] Since then, many other cryptocurrencies have emerged, utilizing the same innovation that Bitcoin introduced but with modified algorithms. Cryptocurrency operates on a peer-to-peer mechanism, where the exchange of currency is not governed by a central bank authority. In other words, in cryptocurrency transaction models, third parties are not involved in the exchange process.

Cryptocurrency, as previously described in terms of its features, has, in the author's view, a high potential to be used as a modus operandi for crimes. This is particularly due to one of its primary characteristics, which allows transactions to be conducted on a peer-to-peer basis without the involvement of a third party—typically the state—to oversee and regulate these transactions. As a result, the role of the state and other intermediaries is effectively eliminated within this framework. Additionally, cryptocurrency mechanisms facilitate anonymous transactions by allowing users to operate under fictitious identities. These transactions are further protected by complex cryptographic encryption, which is claimed to be equivalent to military-

32 David Chaum, "Blind Signatures For Untraceable Payments," Springer-Verlag, 1998, 199–203.

33 Eli Dourado And Jerry Brito, "Bitcoin - Solving Double Spending," The New Palgrave Dictionary Of Economics, No. Online Edition (2014).

34 Malcolm Campbell-Verduyn, "Bitcoin; Crypto-Coins; Financial Action Task Force; Global Governance; Money Laundering H," Crime, Law And Social Change, 2017, 1–30.

grade encryption standards. Given that Indonesia is embracing the Fourth Industrial Revolution (Industry 4.0), it is inevitable that cryptocurrency mechanisms will emerge as a consequence of this technological shift. Therefore, a comprehensive study of cryptocurrency mechanisms and their impact on various aspects, including the legal domain, is necessary. This paper specifically focuses on an analysis of Indonesia's criminal law system[35] concerning the criminal risks posed by cryptocurrency mechanisms. According to L.M. Friedman, the legal system consists of four main elements: legal structure, legal substance, legal culture, and legal impact.[36] In examining the criminal potential of cryptocurrency mechanisms, this study will focus on three key elements within Indonesia's criminal law system: legal substance, legal structure, and legal impact, in the context of addressing the criminal risks associated with cryptocurrency.

A.2 Legal Substance and the Potential of Cryptocurrency Crimes

The study and analysis related to legal substance in this paper will examine the types of crimes that may arise from cryptocurrency mechanisms and the regulations that govern these potential crimes. **Firstly**, the focus will be on cryptocurrency mechanisms and the potential for money laundering. The author's argument explores the relationship between cryptocurrency mechanisms and the potential for money laundering, considering that the misuse of cryptocurrency mechanisms as a medium for committing crimes holds the greatest potential for such offenses. Money laundering is an organized crime defined as the process by which an individual consolidates the existence,

---

35 Indonesia's Criminal Law System Is An Integrated Framework Composed Of Interrelated Components Working Within A System To Achieve Its Objectives. The Criminal Law System Is A Public Law System Consisting Of: Material Law (The Criminal Code, Non-Codified Criminal Laws, And Penal Provisions In Regional Regulations) And Formal Law (Criminal Procedure Code, Special Procedural Criminal Laws Beyond The Criminal Procedure Code). See Edward Omar Sharif Hiariej, "Asas Lex Specialis Systematis Dan Hukum Pidana Pajak," Jurnal Penelitian Hukum De Jure 21, No. 1 (2021): 1–12.

36 Slamet Tri Wahyudi, "Problematika Penerapan Pidana Mati Dalam Konteks Penegakan Hukum Di Indonesia," Jurnal Hukum Dan Peradilan 1, No. 2 (2012): 207, Https://Doi.Org/10.25216/Jhp.1.2.2012.207-234.

illegal sources, or the illicit application of income, and then disguises it to make it appear as though it originates from legitimate sources.[37] Under the Indonesian criminal law, this matter is specifically addressed in Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering. Article 2(1) of the Anti-Money-Laundering Law lists 26 predicate offences; although "cryptocurrency" is not named, crypto-related wrongdoing can still fit within several existing rubrics, for example, fraud, corruption, banking crimes, or the residual clause covering any offence punishable by four years or more—so prosecutors may interpret digital-asset schemes as valid predicates for money-laundering charges.

However, the use of cryptocurrency as a modus operandi for the crime of money laundering is not explicitly mentioned in the provisions of Article 2, paragraph (1). This omission can lead to legal uncertainties, particularly regarding how cryptocurrency can be misused as a mechanism for committing money laundering offenses, while the existing regulations do not explicitly address this issue. The author acknowledges that cryptocurrency is not explicitly classified as a predicate offense for money laundering under the law. This is understandable, considering that at the time Law Number 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering was enacted, cryptocurrency was not yet widely recognized and, therefore, was not considered by legislators. Nonetheless, the author seeks to objectively analyze the legal provisions related to money laundering that may be applicable to the misuse of cryptocurrency as a modus operandi for such crimes. It cannot be conclusively stated that all existing legal provisions are entirely inapplicable to preventing this crime. One provision that the author believes could be applied to the misuse of cryptocurrency as a means of money laundering is Article 3, which states that:

---

37 President's Commission On Organized Crime, "The Cash Connection: Organized Crime, Financial Institutions, And Money Laundering," Interim Report To The President And The Attorney General, Vol. 1 (Washington, D.C, 1984).

> *"Any person who deposits, transfers, assigns, spends, pays, donates, entrusts, moves abroad, alters the form, exchanges for currency, securities, or other assets—while knowing or reasonably suspecting that these assets originate from a criminal act as referred to in Article 2, paragraph (1)—with the intent to conceal or disguise their origin, shall be subject to punishment for the crime of money laundering. The penalty includes a maximum prison sentence of 20 (twenty) years and a maximum fine of IDR 10,000,000,000.00 (ten billion rupiah)."*

The author's argumentative basis asserts that the provisions can be applied to the misuse of cryptocurrency mechanisms for money laundering by employing the "*argumentum per analogiam* method"[38] This is based on the interpretation that Article 2, paragraph (1), letter z allows for the inclusion of other similar crimes that carry criminal penalties, even if they are not explicitly mentioned as predicate offenses.

However, returning to the fundamental issue of whether Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes adequately addresses the use of cryptocurrency, the author emphasizes that the law is insufficient. This inadequacy arises from the fact that cryptocurrency is not expressly recognized as a predicate offense for money laundering, creating potential opportunities for decriminalization in such cases. Given the unique characteristics of cryptocurrency—previously discussed by the author—which provide avenues for criminal activities, relying solely on Article 3 for prevention and enforcement is impractical. The application of Article 3 in this context would require an *argumentum per analogiam* approach, which contradicts one of the fundamental

38 In This Analogy, Specific Laws Are Elaborated Into General Laws That Are Not Explicitly Written In Legislation And Are Derived From General Provisions To Address Specific Events. Consequently, A Legal Provision May Apply To A Particular Case That Is Not Explicitly Regulated In The Law, Provided That The Case Is Identical Or Substantially Similar To One That Is Specified In The Legislation. See Soedikno Mertukusumo, Penemuan Hukum Sebuah Pengantar : Cetakan Ke-5 (Yogyakarta: Liberty, 2007); Compare To David Hardiago And Syafrinaldi, "Asas Legalitas Dan Self Plagiarism: Antinomi Realitas Empiris Sebagai Proyeksi Pengaturan Tindak Pidana Khusus Di Bidang Hak Cipta," Uir Law Review 6, No. 2 (2023): 01–23, Https://Doi.Org/10.25299/Uirlrev.2022.Vol6(2).11689.

principles of criminal law: the specificity of crime definitions and penalties.[39] Thus, it can be concluded that the current legal provisions on money laundering are inadequate in addressing the cryptocurrency mechanism. This inadequacy not only weakens enforcement but also creates opportunities for crimes to be committed through cryptocurrency in the context of money laundering.

Second, Cryptocurrency Mechanisms and the Potential for Tax Evasion. In this section, the author distinguishes between tax evasion and the proceeds of tax-related offenses as set forth in Article 2(1) of the Money Laundering Act. The justification for separating these discussions arises from the complexity and the importance of examining, in-depth, how cryptocurrency mechanisms might facilitate tax evasion. Moreover, in the author's view, the nature of the tax evasion addressed here differs from taxation offenses encompassed by the Money Laundering Act. To clarify this distinction, one may note that in tax crimes under the Money Laundering Act, illicit proceeds are made to appear lawful through money-laundering techniques, indicating that the assets were illegal from the outset. In contrast, the tax evasion discussed here involves legitimate assets that are placed into digital currency via cryptocurrency mechanisms as a way to circumvent tax obligations, resulting in lost tax revenue for the state. Additionally, the separation of these topics reflects concerns over how taxes are levied on transactions utilizing cryptocurrency and the potential criminal implications that may arise if there is no adequate legal framework to address these issues.

Nonetheless, the author fully recognizes that the distinction posited above is not intended as an absolute demarcation. The legal analysis advanced in this study emerges from an interconnected legal framework, rendering a strict separation impracticable. Indonesia's tax regime is primarily governed by Law Number 16 of 2009, which ratifies the Government Regulation in Lieu of Law Number 5 of

---

39 Eddy O.S Hiariej, Prinsip-Prinsip Hukum Pidana: Edisi Revisi, 2nd Ed. (Yogyakarta: Cahaya Atma Pustaka, 2016); David Hardiago, "Delik Politik Dalam Hukum Pidana Indonesia," Jurnal Hukum & Pembangunan 50, No. 4 (2021): 908, Https://Doi.Org/10.21143/Jhp.Vol50.No4.2859.

2008 concerning the Fourth Amendment to Law Number 6 of 1983 on General Tax Provisions and Procedures (hereinafter referred to as the KUP Law). In essence, the KUP Law delineates the mechanisms through which the state calculates and collects taxes from taxable subjects by means of three principal systems: Self-Assessment System, whereby taxpayers themselves bear the responsibility for calculating, remitting, and reporting their tax obligations. Official Assessment System, whereby the authority to determine the amount of tax owed rests with the fiscal apparatus or tax officials. Withholding System, whereby a third party—distinct from both the taxpayer and tax authorities—calculates and remits the applicable taxes.[40]

Next, in light of Indonesia's tax regulations and collection systems, the author aims to determine whether these frameworks can effectively prevent tax evasion facilitated through cryptocurrency. To illustrate this, the author presents a simple demonstrating how the KUP Law might apply. Within the cryptocurrency ecosystem, numerous digital currencies offer distinct features. For this illustration, the author chooses XMR Monero[41] which not only employs a decentralized transaction mechanism (common to most cryptocurrencies) but also provides an "invisible" feature. This means the transaction details—including the identities of the sender and the recipient—are untraceable, the contents of the wallet remain hidden, and the cryptographic protocols are exceedingly complex, all while maintaining a user-friendly interface.

Case illustration. Assume **A** is an individual Indonesian tobacco entrepreneur who earns **IDR 100,000,000,000** (one hundred billion rupiah) in profits. Under **Law Number 36 of 2008 on Income Tax**, A's tax liability would be calculated as follows:

---

40 Zeny Jayanti, Fadjar Harimurti, And Djoko Kristianto, "Pengaruh Self Assessment System Dan Pemeriksaan Pajak Terhadap Penerimaan Pajak Pertambahan Nilai (Studi Pada Kpp Pratama Boyolali Tahun 2013 – 2018)," Jurnal Akuntansi Dan Sistem Teknologi Informasi 15, No. 1 (2020): 114–22, Https://Doi.Org/10.33061/Jasti.V15i1.3671.

41 Olivia Angela et al., "Faktor-Faktor Yang Mempengaruhi," n.d. Https://Core.Ac.Uk/Outputs/328807841/?Utm_Source=Pdf&Utm_Medium=Banner&Utm_Campaign=Pdf-Decoration-V1. P. 7. Accessed On 20 December 2024 At 19:20

Total profit = 100.000.000

Personal Exemption: not married and no dependents, pursuant to Article 7 of the Income Law tax

(TK/0) = 54.000.000(-)

Taxable income (Article 17 Income Law Tax)

= 100.000.000 – 54.000.000 = 99.946.000.000

Applicable income tax (Article 17(1) of the Income Tax Law)

5% X 50.000.000= 2.500.000

15% X 200.000.000= 30.000.000

25% X 250.000.000= 29.833.800.000(+)

Total income tax payable = **Rp. 29.928.800.000**

From these calculations, A is required to pay IDR 29,928,800,000 in income tax (PPh) to the Indonesian government. However, A deems that the assessed tax liability is too high. Consequently, A utilizes the XMR Monero cryptocurrency mechanism to channel all of his profits, aiming to evade taxation on his earnings. In addition, A hires a personal accountant to fabricate the company's financial records in a manner that suggests the business is operating at a loss, thereby circumventing external audits.

Furthermore, one may inquire how the KUP Law would function in circumstances resembling the illustrative scenario. In theory, the state, through its tax authorities, could conduct an external audit, potentially uncovering suspicious transactions carried out by A based on the accountant's records. However, the question remains whether evidence of suspicious transactions derived from these records could be pursued under the KUP Law to establish tax evasion. In the author's view, considering the example discussed and the current provisions of the KUP Law, the law appears inadequate to fully address

such complexities. The author's reasoning is grounded in several considerations, the first of which is encapsulated in the maxim "het recht hinkt achter de feiten aan," meaning "the law inevitably lags behind real-world events.[42]

This perspective aligns with the evident obsolescence of the current KUP Law, as the amendments made to Law No. 6 of 1983 have primarily focused on selective provisions rather than providing a comprehensive revision that would adequately address the evolving legal landscape (constituting a partial reformulation). Furthermore, while an online tax collection mechanism is in place, it predominantly utilizes alternative payment methods, rather than addressing the taxation of transactions conducted via cryptocurrency mechanisms—a potential revenue stream for the state that remains largely unregulated. This gap underscores the necessity for a more integrated and forward-looking legal framework that accounts for the complexities of modern financial technologies within the national tax system.

Secondly, the author believes that the current provisions of the KUP Law do not explicitly regulate the burden of proof in cases of tax evasion facilitated through cryptocurrency mechanisms. This is of particular importance given that tax evasion via cryptocurrency is not only easily exploited as a modus operandi for criminal activity but also poses significant challenges for tax auditors when suspicious transactions are detected. Additionally, the principle of law in burden of proof—"actori incumbit probatio, actori incumbit onus probandi, actore non probante, reus absolvitur" (which means, "he who asserts must prove, he who claims his right must prove, and if the defendant does not prove, they must be acquitted")—stipulates that when the state seeks to enforce its rights to tax revenue, it is incumbent upon the state to provide evidence of the offense. This principle makes the situation particularly challenging, as the current KUP Law does not clearly regulate the burden of proof in the context of cryptocurrency-

42 David Hardiago And Syafrinaldi Syafrinaldi, "Terorisme Dan Pemasyarakatan: Problem Hukum Pendidikan Deradikalisasi Bagi Terpidana Terorisme Di Indonesia," Jkih : Jurnal Kajian Ilmu Hukum 1, No. 2 (2022): 146–75, Https://Doi.Org/10.55583/Jkih.V1i2.294.

related tax evasion. This regulatory gap is further compounded by the fact that cryptocurrency mechanisms are not explicitly addressed in the existing law. Therefore, it can be concluded that the current legal framework regarding tax evasion related to cryptocurrency is insufficient, and this lack of clarity and regulation presents both a significant challenge for law enforcement and an opportunity for criminal exploitation in the realm of tax evasion facilitated by cryptocurrency.

A.3 Legal Structure and the Indications of Cryptocurrency-Related Crimes

The legal issues associated with the potential crimes arising from cryptocurrency mechanisms within Indonesian criminal law are not merely a matter of legal substance. In the author's view, an examination of the legal structure is also necessary to understand how prepared Indonesia's legal system is to prevent and address the potential crimes associated with cryptocurrency. Furthermore, within the framework of "the criminal justice system"[43] the role of relevant legal institutions that handle criminal cases involving cryptocurrency mechanisms significantly impacts the effectiveness of criminal case management. Currently, Indonesia lacks a dedicated legal institution specifically tasked with addressing crimes involving cryptocurrency mechanisms. Indonesia has no stand-alone agency for crypto-asset crimes, but this gap could be filled by upgrading the PPATK's cyber-intelligence unit into a dedicated "Crypto-Asset Financial Intelligence Centre," mandated to trace, freeze, and forfeit digital funds, while pairing it with a joint task-force that links PPATK analysts, Bappebti market-supervisors, and a new Cyber-Currency Crime Directorate within the National Police, an arrangement that

43 The Criminal Justice System Is A System Deliberately Established To Implement Law Enforcement Efforts (Criminal Law), Where Its Execution Is Constrained By Specific Operational Mechanisms Within A Set Of Legal Procedural Rules. See Ferdian Rinaldia, "Proses Bekerjanya Sistem Peradilan Pidana Dalam Memberikan Kepastian Hukum Dan Keadilan," Jurnal Hukum Respublika vol 21 (2022): 179–188.

would unify licensing oversight, real-time market surveillance, and criminal investigation under one coordinated framework.

This gap is not only the result of the cryptocurrency mechanisms being relatively new to the country but also reflects the underdeveloped understanding of how cryptocurrencies can be exploited as a modus operandi for crime. Moreover, the growing awareness of the need to address cryptocurrency-related issues has only emerged after Indonesia's government projected the entry into Industry 4.0, which will inevitably be followed by a massive adoption of cryptocurrency. This transition emphasizes the urgency for Indonesia to adapt its legal structure to effectively manage the risks posed by cryptocurrency-related crimes.

Another argument supporting the absence of a dedicated institution for addressing cryptocurrency-related crimes in Indonesia is the lack of legal recognition for digital currencies in the country, as evidenced by the overlapping regulatory recognition of such currencies.[44] According to Bank Indonesia regulations, such as Article 34 of Bank Indonesia Regulation No. 18/40/PBI/2016 on the Implementation of Payment Transaction Processing and Articles 8(1) and 8(2) of Bank Indonesia Regulation No. 19/12/PBI/2017 on the Implementation of Financial Technology, the central bank explicitly prohibits all payment system providers (including principals, switching operators, clearing operators, settlement providers, issuers, acquirers, payment gateways, e-wallet operators, and fund transfer providers), as well as financial technology providers in Indonesia—both banks and non-bank institutions—from processing virtual currency payments. This regulatory stance reflects Bank Indonesia's authority in the monetary sector, with the goal of maintaining financial system stability, protecting consumers, and preventing money laundering and terrorism financing. However, the lack of clarity surrounding the legal status of virtual currencies further complicates the situation and

[44] Ida Ayu Samhita Chanda Thistanti, I Nyoman Gede Sugiartha, and I Wayan Arthanaya, "Kajian Yuridis Mengenai Legalitas Cryptocurrency Di Indonesia," *Jurnal Preferensi Hukum* 3, no. 1 (2022): 7–11, https://doi.org/10.22225/jph.3.1.4592.7-11.

underscores the need for comprehensive regulatory frameworks to address the growing use of cryptocurrency mechanisms in financial transactions and potential criminal activities.[45]

The Bank Indonesia regulations can be interpreted considering the ratio legis underlying these provisions, grounded in Article 1(1) of Law No. 7 of 2011 on Currency, which defines currency as "Money issued by the Republic of Indonesia, hereinafter referred to as the Rupiah." Accordingly, expressly, Article 21(1) of the same law stipulates that "Any transaction aimed at payment, or any other obligation to be fulfilled with money, or other financial transactions conducted within the territory of the Republic of Indonesia, must use Rupiah." This provision explicitly prohibits the use of cryptocurrency as a means of payment, transaction, or fulfillment of any obligations within Indonesia's jurisdiction.

In contrast, Article 1 of Ministry of Trade Regulation No. 99 of 2018 on Crypto Assets explicitly acknowledges and designates crypto assets as commodities that may be used in futures contracts traded on futures exchanges. This regulation is further elaborated through technical provisions, such as BAPPEBTI Regulation No. 3 of 2019 concerning Commodities Eligible for Futures Contracts, Sharia Derivative Contracts, and/or Other Derivative Contracts Traded on Futures Exchanges, and BAPPEBTI Regulation No. 5 of 2019 on the Technical Provisions for the Organization of Physical Crypto Asset Markets on Futures Exchanges. These regulations issued by the Ministry of Trade clearly recognize cryptocurrency as an asset that can be utilized in transactions, particularly in investment activities within Indonesia.

The absence of legal recognition and the overlapping acknowledgment of cryptocurrency in Indonesia will undoubtedly affect the establishment of state institutions specifically responsible for handling crimes arising from cryptocurrency mechanisms. This is

---

45 Agusman, "Bank Indonesia Warns All Parties Against Selling, Buying, or Trading Virtual Currency," Bank Indonesia, 2018.

particularly significant considering the principles of subjective criminal law (jus puniendi), which grant the state the right to impose criminal sanctions, including prosecution, sentencing, and enforcement of penalties. However, the exercise of such powers within the scope of subjective criminal law cannot be carried out effectively without objective criminal law, which serves to limit the state's authority and provide a legal framework to ensure due process and fairness in the enforcement of criminal penalties.[46] This indicates that within the Indonesian criminal justice system, the lack of legal provisions regulating and recognizing the status of cryptocurrency not only results in the absence of a specialized institution to address crimes associated with cryptocurrency mechanisms but also creates significant challenges in the enforcement of law when such crimes occur. This situation is compounded by the fact that, without a dedicated legal framework, it is difficult to manage and respond to crimes facilitated by cryptocurrency mechanisms.

Ideally, as per the Anti-Money Laundering Law (UU TPPU), a specialized institution for handling crimes related to suspicious transactions has been established. This institution is the Financial Transaction Reports and Analysis Center (PPATK). However, in reference to PPATK Regulation No. 11 of 2013 on the Identification of Suspicious Financial Transactions for Financial Service Providers, the establishment of PPATK is specifically intended for the handling of suspicious transactions in the context of money laundering offenses. Additionally, the regulation stipulates that the identification of Suspicious Financial Transactions (TKM) is the responsibility of the financial service providers, who are required to submit documents including user profiles, transaction records, monitoring systems, and user lists. Applying this identification mechanism to cryptocurrency transactions presents significant challenges, as the very appeal and key

46 Edward Omar Sharif Hiariej, "Asas Lex Specialis Systematis Dan Hukum Pidana Pajak," *Jurnal Penelitian Hukum De Jure* 21, no. 1 (2021): 1–12.

feature of cryptocurrency mechanisms lie in their anonymity,[47] and the confidentiality of transactions, which are protected by complex cryptographic encryption.[48] Consequently, the existing legal structure, particularly the absence of a specialized institution to handle crimes related to cryptocurrency in the Indonesian criminal justice system, is clearly inadequate. In conclusion, the lack of an appropriate legal structure, as outlined by the arguments above, contributes significantly to the potential for cryptocurrency-related crimes in Indonesia. This gap in the legal framework is a critical factor that enables the perpetration of such crimes and underscores the need for specialized legal reforms to address the complexities of cryptocurrency in the criminal justice system.

Based on the discussion of the substance and the legal structure of criminal law in Indonesia in relation to the potential crimes facilitated by cryptocurrency mechanisms, the following conclusions can be drawn: First, the misuse of cryptocurrency mechanisms can lead to potential crimes in the context of money laundering and tax evasion, as viewed through the current legal framework in Indonesia. Second, the lack of clarity regarding the legal status of cryptocurrency in Indonesia can result in the absence of a legal structure, particularly the lack of a dedicated institution with the authority to address such crimes. Third, the potential criminal activities facilitated by cryptocurrency can have significant implications for the country's economy. This is particularly concerning since the misuse of cryptocurrency directly relates to economic crimes, which, in this paper, the author focuses on money laundering and tax evasion as examples. However, a more comprehensive examination reveals that the potential crimes stemming from cryptocurrency mechanisms extend beyond money laundering and tax evasion. These mechanisms can also be exploited as a **modus operandi** for other crimes, including terrorism financing, human

---

47 Syahrul Sajidin, "Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran Di Indonesia," Arena Hukum 14, no. 2 (2021): 245–267, https://doi.org/10.21776/ub.arenahukum.2021.01402.3.

48 Nurul Huda and Risman Hambali, "Risiko Dan Tingkat Keuntungan Investasi Cryptocurrency," *Jurnal Manajemen Dan Bisnis: Performa* 17, no. 1 (2020): 72–84.

trafficking, illegal trade (such as drugs, weapons, etc.), and various other criminal offenses.

B. Prevention and Mitigation of Cryptocurrency Crimes through Criminal Policy

The increasing use of cryptocurrencies has led to significant challenges for criminal justice systems worldwide, including Indonesia,[49] from the author's perspective, this presents a significant potential for abuse as a new modus operandi for criminal activity, as discussed in previous sections. Therefore, it is crucial to seek solutions that can serve as projections for anticipating crimes on one hand, and, on the other hand, as effective measures to address and mitigate these crimes once they have occurred.

The projection for anticipating crimes within the framework of criminal law, particularly in terms of law enforcement mechanisms, can ideally be addressed through non-penal policy measures, such as various preventive efforts, without necessarily resorting to the criminal justice system.[50] However, given the lack of legal regulations regarding the use of cryptocurrency, the solution proposed is to utilize penal policy mechanisms to anticipate and address the potential crimes resulting from the use of cryptocurrency. The penal policy suggested here can be understood as both a science and an art, with the ultimate practical aim of formulating positive legal regulations more effectively. It serves not only to guide lawmakers but also provides direction for those responsible for

---

49 Fatmalina Kharisma, "Evaluasi Pemanfaatan Regulatory Technology Dalam Sistem Anti-Pencucian Uang Untuk Aset Virtual Di Indonesia," Magister Akutansi Fakultas Bisnis Dan Ekonomika (Thesis, Universitas Islam Indonesia, 2024).

50 As An Example Of Criminal Policy, Efforts Include Mental Health Improvement Programs For Society, Legal Education, And Other Preventive Measures. Additionally, Non-Penal Policies Are Considered More Strategic Than Penal Policies. This Is Because Non-Penal Policies Are More Preventive In Nature, With The Primary Goal Of Eliminating The Conducive Factors That Lead To Crime, As Emphasized In The United Nations Congress On The Prevention Of Crime And The Treatment Of Offenders. SeeSupriyadi, "Bahan Ajar Kebijakan Hukum Pidana" (Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2018).

implementing court decisions, consisting of criminology, criminal law, and penal policy itself.[51]

In this context, the author will focus the analysis on the formulation stage of penal policy. This stage is the most strategic and foundational phase, as it forms the basis and provides the guidelines for both the application and execution stages. Therefore, errors or weaknesses at the formulation stage can serve as obstacles during the application and execution phases.[52] However, in the realm of criminal law policy, particularly during the formulation stage, central issues remain unresolved. The first issue pertains to defining which acts should be prohibited and designated as criminal offenses. The second issue is related to determining the appropriate sanctions to impose on the offenders. To address these central issues related to crimes arising from cryptocurrency mechanisms, the author applies the criteria established at the National Symposium on Criminal Law Reform in August 1980 in Semarang, which includes both general and specific criteria, explained as follows.

B.1 Acts that are Condemned by Society and Cause Harm to Victims

Cryptocurrency, as a mechanism with significant potential for misuse, can serve as a modus operandi for criminal activities, thereby impacting the criteria outlined in the first parameter. Given its function as a tool for committing crimes, cryptocurrency inevitably causes financial losses and produces victims. Its greatest risk of misuse lies in its application as a medium for economic crimes, particularly money laundering and tax evasion, regardless of individual victims. The misuse of cryptocurrency is likely to result in widespread and multidimensional harm, similar to other offenses in the financial sector.

---

51 Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Prenada Media Group, 2008).

52 Wenggedes Frensh, "Kelemahan Pelaksanaan Kebijakan Kriminal Terhadap Cyberbullying Anak Di Indonesia," *Indonesia Criminal Law Review* 1, no. 2 (2022): 87–99.

From this perspective, the misuse of cryptocurrency as a criminal modus operandi would likely be followed by negative societal stigma. Acts that cause harm and victimize individuals or institutions are generally condemned by society, and such societal disapproval often serves as a driving factor in the formation of legislative policies, particularly in Indonesia. However, at present, the direct public reaction to cryptocurrency-related crimes has yet to be fully realized as its impact remains relatively indirect and less apparent. For instance, in the United States, legislative efforts are underway to develop a specialized legal framework to address cryptocurrency-related offenses. This trend highlights the increasing recognition of cryptocurrency as a tool for financial crime and underscores the need for further research into how Indonesia should respond legislatively to mitigate these risks effectively.

B.2 Cost-Benefit Analysis

In this second parameter, the author seeks to examine two key aspects: First, an analysis of the costs and outcomes associated with the criminalization of cryptocurrency misuse as a modus operandi for financial crimes. Second, an exploration of the *ius constituendum* projection as a framework for mitigating the potential risks posed by such offenses.

Focusing on the first point of discussion, the author begins by evaluating the implications of cryptocurrency misuse, as previously outlined, which presents a significant risk of being exploited for economic crimes, particularly money laundering and tax evasion. In the Indonesian context, the total transaction volume of digital currencies, such as Bitcoin, which represents just one among many digital assets within the cryptocurrency ecosystem, has already reached IDR 4 billion per day. This substantial volume underscores the urgency of establishing a comprehensive legal framework to regulate

and mitigate the risks associated with cryptocurrency transactions.[53] The high volume of cryptocurrency transactions combined with minimal government oversight due to the current regulatory vacuum creates a significant risk of misuse for illicit activities, including money laundering, tax evasion, and other financial crimes. Such vulnerabilities could have profound implications for the national economy. Although the direct impact of cryptocurrency on Indonesia's financial stability has not yet been fully realized, the concerns raised by Bank Indonesia, as the institution responsible for maintaining the country's financial stability, highlight the potential for cryptocurrency mechanisms to be exploited as a modus operandi for criminal activities. These concerns serve as an early warning of the economic risks that Indonesia may face in the future if regulatory measures are not proactively implemented.[54]

Thus, the author contends that the legislative codification of cryptocurrency-related offenses, as a mechanism of criminalization, represents a pragmatic and necessary approach to addressing such crimes. This perspective is further reinforced by the fact that the enactment of a single statute in Indonesia entails an average fiscal outlay of approximately IDR 6.56 billion.[55] Such legislation, if effectively designed to combat cryptocurrency-related crimes and to grant legal authority to existing institutions tasked with addressing these offenses, would remain applicable for an extended period. The substantial expenditure required for drafting a single law is insignificant when

---

53 Finna U Ulfah, "Semester 1/2019, Tokocrypto Cetak Volume Transaksi Rp4 Miliar per Hari," Bisnis.Com, July 2019. Https://Www.Google.Co.Id/Amp/S/M.Bisnis.Com/Amp/Read/20190703/94/1119611/Semester-12019-Tokocrypto-Cetak-Volume-Transaksi-Rp4-Miliar-Per-Hari Accessed On 20 December 2024 At 19:20 Wib.

54 Andhira Wardani, Mahrus Ali, and Jaco Barkhuizen, "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act," *Lex Publica* 9, no. 2 (2022): 49–66, https://doi.org/10.58829/lp.9.2.2022.49-66.

55 Dwi Hadya Jayani, "Berapa Anggaran Legislasi DPR Periode 2014-2019?," Katadata Media Network, 2019. Https://Databoks.Katadata.Co.Id/Datapublish/2019/10/01/Berapa-Anggaran-Legislasi-Dpr-Periode-2014-2019 Accessed On 20 December 2024 At 19:20 Wib.

compared to the monthly Bitcoin transaction volume in Indonesia, which reaches approximately IDR 120 billion.

Moreover, the criminalization of cryptocurrency-related crimes through legislative enactment would not only establish a formal legal framework governing cryptocurrency transaction but also generate additional state revenue if the statute includes provisions for taxation on cryptocurrency transactions. This raises a critical question: How should the projected legal framework be structured? Given that cryptocurrency mechanisms as a modus operandi for crime intersect with multiple existing legislative provisions in Indonesia, the development of a comprehensive and harmonized legal framework becomes a pressing necessity.

To effectively address this issue, the author examines the second discussion point, which explores the projection of ius constituendum as a prospective legal framework for mitigating the criminal risks associated with cryptocurrency mechanisms. Beyond the initial proposal for criminalization through legislative enactment as a preventive measure, a critical aspect warranting further examination is the ideal structure and conceptualization of the envisioned legal framework. This necessity arises from the fact that cryptocurrency-related criminal threats extend beyond multiple existing legislative provisions, while there remains a notable absence of a dedicated regulatory framework or specialized institution to comprehensively govern such matters. Accordingly, the author advocates for the formulation of a specialized legal framework (lex specialis), meticulously designed to establish robust regulatory oversight and effectively address the multifaceted legal challenges posed by cryptocurrency transactions.

The author's argument is based on the following: Firstly, although the potential crimes arising from cryptocurrency mechanisms currently involve multiple legislative regulations, considering the large number of draft legislative regulations included in the National

Legislation Program (Prolegnas),[56] and the existing legal instruments in Indonesia, it is necessary to implement partial reform of the relevant laws by establishing a single specialized legislative framework that regulates and complements the existing provisions. Secondly, the emphasis on state budget efficiency, particularly if partial reformulation of various regulations related to cryptocurrency-related crimes were to be carried out. This is a crucial consideration, given that the formation of a single regulation in Indonesia currently costs an average of IDR 6.3 billion. Thirdly, the need to reduce potential regulatory overlap. The large number of legislative products increases the risk of redundant and conflicting regulations governing the same subject matter.

Another central issue in penal policy concerns the substantive provisions and the determination of criminal sanctionswithin the proposed special legislation. Given the complexity of this matter, further research is essential to ensure a well-grounded and effective regulatory framework. The author acknowledges that the drafting of any legislative proposal necessitates the involvement of a team of experts and comprehensive research to establish both the substantive content and the appropriate scope of criminal sanctions. This meticulous approach is crucial to ensuring that the legislative framework adequately addresses the risks associated with cryptocurrency-related offenses. In this regard, the determination of sanctions in legislative policy must consider three key aspects: Firstly, types of criminal sanctions (strafsoort), establishing the appropriate classification of offenses related to cryptocurrency transactions, whether as criminal offenses subject to imprisonment or regulatory violations subject to administrative sanctions. *Strafsoort* should draw a clear line between genuinely criminal behaviour and market-conduct breaches. Core wrongdoing, such as laundering proceeds through crypto wallets, funding terrorism with digital assets, or running

[56] Dewan Perwakilan Rakyat Republik Indonesia (DPR-RI), "In the National Legislative Program (Prolegnas) for 2020–2024, a Total of 248 Draft Laws Have Been Registered. ," Source: http://www.dpr.go.id/uu/prolegnas, 2020.

fraudulent "rug-pull" token offerings, must remain criminal offences triable under the Law No. 5 of 2018 on Eradication of Criminal Act of Terrorism and UU TPPU. By contrast, failures to obtain a licence, keep proper Know-Your-Customer (KYC) records, or submit suspicious-transaction reports should be treated as administrative violations enforced by Bappebti or, where the entity offers quasi-banking products, the PPATK and OJK. This dual track mirrors Indonesia's existing separation between "hard" crimes (e.g., corruption, narcotics) and supervisory breaches (e.g., banking-licence lapses), providing both clarity and proportionality.

Secondly, severity of criminal Sanctions (strafmaat), defining the range and proportionality of penalties based on the nature and gravity of cryptocurrency-related crimes, particularly in cases involving money laundering, fraud, tax evasion, or terrorism financing. *Strafmaat* must be tied to the gravity of each offence class while respecting the ceiling and floors already rooted in Indonesian law. For money-laundering and crypto-based terrorism financing, the recommended band is five to twenty years' imprisonment plus fines up to IDR 10 billion, echoing Articles 3–4 of the UU TPPU. Fraudulent token sales or initial-coin-offering scams—viewed as aggravated forms of conventional fraud under a new proposed regulation that specifically regulate —would attract four to twelve years' jail and fines up to IDR 8 billion. Crypto-mediated tax evasion should follow Article 39 of the UU KUP, warranting two to six years' imprisonment and a fine of 300 percent of the unpaid tax. At the administrative tier, unlicensed exchange operation or KYC lapses would trigger escalating measures: written warnings, temporary suspension, licence revocation, and fines ranging from IDR 500 million to IDR 5 billion—allowing regulators to calibrate punishment without criminalising every compliance slip.

Lastly, methodes of Enforcement (strafmodus), determining the most effective mechanisms for implementing criminal sanctions, including asset seizure, financial penalties, and international

cooperation for transnational offenses.[57] Strafmodus must combine rapid preventive measures with effective cross-border cooperation. The authority to include new ones is carried out after the legal subject is proven and sentenced to a criminal penalty as stipulated in strafmaat and strafmodus which have been previously regulated in the TPPU Law. However, considering that cryptocurrency as a modus operandi has not been regulated before, the offer of strafmodus for the crime will include confiscating private keys, wallets, NFTs, and other virtual assets, while the proposed "Crypto Asset Financial Intelligence Center" at PPATK can issue on-chain freezing orders for 24 hours in a remote period that can be extended until the conference is completed, as well as coordinate blockchain analysis, and provide actionable intelligence to the new Cybercrime Directorate at the National Police. For transnational cases, Indonesia must expedite requests for mutual legal assistance and recognize foreign inclusion orders from FATF-compliant recognition, ensuring that borderless assets meet borderless justice. On the administrative side, unpaid fines or persistent non-compliance will automatically escalate to criminal offenses, creating a seamless continuum between law enforcement and criminal law enforcement. Together, these calibrated third elements provide Indonesia with a coherent and constitutional framework that punishes serious crypto crimes, deters market misconduct, and provides authorities with the practical tools needed to track, freeze, and seize digital wealth.

B.3 The Capability of Law Enforcement Authorities in Addressing Cryptocurrency-Related Crimes

This section focuses on the competence of law enforcement authorities and examines the impact of enacting specialized legislation to regulate potential crimes facilitated by cryptocurrency on the broader framework of legal structural reform. As previously

57 M Ilham Adepio, "Politik Hukum Penggunaan Sanksi Pidana Penjara Dalam Perundang-Undangan Di Indonesia," Jurnal Ilmiah Kutei 23, no. 2 (2024): 224–45, https://digilib.uin-suka.ac.id/id/eprint/39315/.

discussed, there is currently no dedicated institutional framework specifically established to prevent and combat crimes involving cryptocurrency. In Indonesia, for instance, the Financial Transaction Reports and Analysis Center (PPATK) theoretically possesses the potential to address such threats. However, the absence of legal recognition for cryptocurrency transactions and the lack of a specific legal mandate granting PPATK the authority to intervene in these cases render it ineffective in tackling cryptocurrency-related offenses.

To address this regulatory gap, this author proposes the enactment of a dedicated legal framework governing cryptocurrency-related crimes. Such legislation would catalyze legal structural reform by institutionalizing a specialized enforcement body equipped to prevent and investigate crimes committed through cryptocurrency mechanisms. Nevertheless, given the inherent complexity of cryptocurrency transactions and the uncertainty surrounding the full spectrum of illicit activities they may facilitate, legal structural reform must be comprehensive and methodically executed. This includes developing a recruitment model and training framework to ensure that the proposed enforcement body is staffed with highly qualified and competent human resources capable of effectively mitigating the risks associated with cryptocurrency-enabled financial crimes.

Conclusion

In addressing the legal implications of cryptocurrency use, this research concludes that while cryptocurrency brings transformative benefits to financial systems—such as decentralization and enhanced transactional efficiency—it simultaneously generates serious regulatory and legal dilemmas. The core concern lies in its capacity to obscure user identities and bypass centralized oversight, thereby creating loopholes that can be exploited for economic crimes. These characteristics directly challenge existing legal frameworks, particularly in efforts to combat money

laundering and enforce tax compliance. Ultimately, this study underscores the urgent need for adaptive legal instruments and international cooperation to ensure that the evolution of digital financial systems does not compromise public accountability and economic justice.

References

Adepio, M Ilham. "Politik Hukum Penggunaan Sanksi Pidana Penjara Dalam Perundang-Undangan Di Indonesia." *Jurnal Ilmiah Kutei* 23, no. 2 (2024): 224–45. https://digilib.uin-suka.ac.id/id/eprint/39315/.

Adha, Lalu Adi. "Digitalisasi Industri Dan Pengaruhnya Terhadap Ketenagakerjaan Dan Hubungan Kerja Di Indonesia." *Journal Kompilasi Hukum* 5, no. 2 (2020): 267–98. https://doi.org/10.29303/jkh.v5i2.49.

Agusman. "Bank Indonesia Warns All Parties Against Selling, Buying, or Trading Virtual Currency." Bank Indonesia, 2018.

Ali, Salim Ibrahim, Dr Zuryati, Mohamed Yusoff, Dr Zainal, and Amin Ayub. "Legal Research of Doctrinal and Non-Doctrinal." *International Journal of Trend in Research and Development* 4, no. 1 (May 2017): 2394–9333. www.ijtrd.com.

Angela, Olivia, Finance Program, Yen Sun, and Finance Program. "Faktor-Faktor Yang Mempengaruhi," n.d.

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Prenada Media Group, 2008.

Campbell-Verduyn, Malcolm. "Bitcoin; Crypto-Coins; Financial Action Task Force; Global Governance; Money Laundering H." *Crime, Law and Social Change*, 2017, 1–30.

Chaum, David. "Blind Signatures For Untraceable Payments." *Springer-Verlag*, 1998, 199–203.

Crime, President's Commission on Organized. "The Cash Connection: Organized Crime, Financial Institutions, and Money Laundering." *Interim Report to the President and the Attorney General*. Vol. 1. Washington, D.C, 1984.

Dewan Perwakilan Rakyat Republik Indonesia (DPR-RI). "In the National Legislative Program (Prolegnas) for 2020–2024, a Total of 248 Draft Laws Have Been Registered." Source: http://www.dpr.go.id/uu/prolegnas, 2020.

Dourado, Eli, and Jerry Brito. "Bitcoin - Solving Double Spending." *The New Palgrave Dictionary of Economics*, no. Online Edition (2014).

Dyntu, Valeriia. "Cryptocurrency As A Means Of Money Laundering." *Baltic Journal of Economic Studies* 5, no. 1 (2018): 267–71. https://doi.org/https://doi.org/10.30525/2256-0742/2018-4-5-75-81.

Eddy O.S Hiariej. *Prinsip-Prinsip Hukum Pidana: Edisi Revisi*. 2nd ed. Yogyakarta: Cahaya Atma Pustaka, 2016.

Edward Omar Sharif Hiariej. "Asas Lex Specialis Systematis Dan Hukum Pidana Pajak." *Jurnal Penelitian Hukum De Jure* 21, no. 1 (2021): 1–12.

'Fathi, M' "Al-Shammar, bin Saud M" "Khalifa, Mohamed." "Cryptocurrency and Criminal Liability: Investigating Legal Challenges in Addressing Financial Crimes in Decentralized Systems." *Journal of Money Laundering Control,* 28, no. 3 (May 14, 2025): 504–17. https://doi.org/https://doi.org/10.1108/JMLC-07-2024-0110.

Foley, Sean, Jonathan R Karlsen, Tālis J Putniņš, Itay Goldstein, Wei Jiang, Andrew Karolyi, Michael Weber, and David Easley. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *," n.d. http://www.emcdda.europa.eu/attachements.cfm/att_194336_EN_TD3112366ENC.pdf.

Frensh, Wenggedes. "Kelemahan Pelaksanaan Kebijakan Kriminal Terhadap Cyberbullying Anak Di Indonesia." *Indonesia Criminal Law Review* 1, no. 2 (2022): 87–99.

Harahap, Nova Jayanti. "Mahasiswa Dan Revolusi Industri 4.0." *Ecobisma (Jurnal Ekonomi, Bisnis Dan Manajemen)* 6, no. 1 (2019): 70–78. https://doi.org/10.36987/ecobi.v6i1.38.

Hardiago, David. "Delik Politik Dalam Hukum Pidana Indonesia." *Jurnal Hukum & Pembangunan* 50, no. 4 (2021): 908. https://doi.org/10.21143/jhp.vol50.no4.2859.

Hardiago, David, and Syafrinaldi. "Asas Legalitas Dan Self Plagiarism: Antinomi Realitas Empiris Sebagai Proyeksi Pengaturan Tindak Pidana Khusus Di Bidang Hak Cipta." *UIR Law Review* 6, no. 2 (2023): 01–23. https://doi.org/10.25299/uirlrev.2022.vol6(2).11689.

Hardiago, David, and Syafrinaldi Syafrinaldi. "Terorisme Dan Pemasyarakatan: Problem Hukum Pendidikan Deradikalisasi Bagi Terpidana Terorisme Di Indonesia." *JKIH : Jurnal Kajian Ilmu Hukum* 1, no. 2 (2022): 146–75. https://doi.org/10.55583/jkih.v1i2.294.

Huda, Nurul, and Risman Hambali. "Risiko Dan Tingkat Keuntungan Investasi Cryptocurrency." *Jurnal Manajemen Dan Bisnis: Performa* 17, no. 1 (2020): 72–84.

Imelda Bandaso, Trinita, Fransiskus Randa, and Frischa Faradilla Arwinda Mongan. "Blockchain Technology: Bagaimana Menghadapinya? – Dalam Perspektif Akuntansi." *Accounting Profession Journal* 4, no. 2 (2022): 97–115. https://doi.org/10.35593/apaji.v4i2.55.

Jayani, Dwi Hadya. "Berapa Anggaran Legislasi DPR Periode 2014-2019?" Katadata Media Network, 2019.

Jayanti, Zeny, Fadjar Harimurti, and Djoko Kristianto. "Pengaruh Self Assessment System Dan Pemeriksaan Pajak Terhadap Penerimaan

Pajak Pertambahan Nilai (Studi Pada KPP Pratama Boyolali Tahun 2013 – 2018)." *Jurnal Akuntansi Dan Sistem Teknologi Informasi* 15, no. 1 (2020): 114–22. https://doi.org/10.33061/jasti.v15i1.3671.

'Katz, Lily' "Massa, Annie." "FBI Has 130 Cryptocurrency-Related Investigations, Agent Says Trafficking, Drugs, Kidnapping, Ransomware Cases under Review Agency Has Noticed an Increase in Crypto-Related Crimes." Bloomberg, June 28, 2018.

Kharisma, Fatmalina. "Evaluasi Pemanfaatan Regulatory Technology Dalam Sistem Anti-Pencucian Uang Untuk Aset Virtual Di Indonesia." *Magister Akutansi Fakultas Bisnis Dan Ekonomika*. Thesis, Universitas Islam Indonesia, 2024.

Liao, Yongxin, Eduardo Rocha Loures, Fernando Deschamps, Guilherme Brezinski, and André Venâncio. "The Impact of the Fourth Industrial Revolution: A Cross-Country/Region Comparison." *Production* 28, no. January (2018). https://doi.org/10.1590/0103-6513.20180061.

Maria S.W Suwardjono. *Bahan Kuliah: Metodelogi Penelitian Hukum*. Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2014.

———. *Metodelogi Penelitian Ilmu Hukum*. Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2014.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2005.

Mertukusumo, Soedikno. *Penemuan Hukum Sebuah Pengantar : Cetakan Ke-5*. Yogyakarta: Liberty, 2007.

Minnaar, Anthony. "Online 'Underground' Marketplace for Illicit Drugs : The Prototype Case of the DarkWeb Website 'Silk Road.'" *Acta Criminologia : Southern African Journal of Criminology* 30, no. 1 (2017): 23–47. https://www.researchgate.net/publication/333646270.

Muttaqim, Muttaqim, and Desi Apriliani. "Analysis of The Probability of Money Laundering Crimes toward the Development of Crypto-Currency Regulations in Indonesia." *IJCLS (Indonesian Journal of*

Criminal Law Studies) 4, no. 1 (2019): 29–40. https://doi.org/10.15294/ijcls.v4i1.18714.

'Narayanan, Arvind' "Bonneau, Joseph" "Edward, Felten" "Miller, Andrew" "Goldfeder, Steven." *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. 1st ed. Vol. 1. New Jersey: Princeton University Press, 2016.

'Nelson, Mutiara, Febby' "Prosperiani, Maria, Dianita" "Ramadhan, Choky, Risda" "Andini, Priska, Putri." "Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia ." *Journal of Indonesian Legal Studies* 9, no. 1 (May 8, 2024): 89–130.

Puspita Sari, Desty, Muh Ibnu Fajar Rahim Penanganan Aset Kripto Sebagai Barang Bukti, Penanganan Aset Kripto Sebagai Barang Bukti Dalam Perkara Pidana Desty Puspita Sari, Muh Ibnu Fajar Rahim, Kata Kunci, Aset Kripto, and Barang Bukti. "Handling Of Crypto Assets As Evidence In Criminal Cases." *The Prosecutor Law Review* 03, no. 1 (2025). https://bappebti.go.id/pojok_media/detail/11410,.

Rinaldia, Ferdian. "Proses Bekerjanya Sistem Peradilan Pidana Dalam Memberikan Kepastian Hukum Dan Keadilan." *Jurnal Hukum Respublika* vol 21 (2022): 179–88.

Sajidin, Syahrul. "Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran Di Indonesia." *Arena Hukum* 14, no. 2 (2021): 245–67. https://doi.org/10.21776/ub.arenahukum.2021.01402.3.

'Situmorang, Hendro'. "Indonesia's Crypto Trading Soars 335% to Reach $40 Billion in 2024." Jakartaglobe, January 25, 2025.

Soares, Marcelo Negri, and Marcos Eduardo Kauffman. "Industry 4.0: Horizontal Integration and Intellectual Property Law Strategies In England." *Revista Opinião Jurídica (Fortaleza)* 16, no. 23 (2018): 268. https://doi.org/10.12662/2447-6641oj.v16i23.p268-289.2018.

Soerjono Soekamto. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Press, 2015.

Supriyadi. "Bahan Ajar Kebijakan Hukum Pidana." Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, 2018.

Thistanti, Ida Ayu Samhita Chanda, I Nyoman Gede Sugiartha, and I Wayan Arthanaya. "Kajian Yuridis Mengenai Legalitas Cryptocurrency Di Indonesia." *Jurnal Preferensi Hukum* 3, no. 1 (2022): 7–11. https://doi.org/10.22225/jph.3.1.4592.7-11.

Tiwari, Neil. "The Commodification of Cryptocurrency." *Michigan Law Review* 117, no. 3 (2018): 611–34. https://doi.org/10.36644/mlr.117.3.commodification.

Ulfah, Finna U. "Semester 1/2019, Tokocrypto Cetak Volume Transaksi Rp4 Miliar per Hari." *Bisnis.Com*, July 2019.

Vejačka, Martin. "Basic Aspects of Cryptocurrencies," n.d., 75–83.

Wahyudi, Slamet Tri. "Problematika Penerapan Pidana Mati Dalam Konteks Penegakan Hukum Di Indonesia." *Jurnal Hukum Dan Peradilan* 1, no. 2 (2012): 207. https://doi.org/10.25216/jhp.1.2.2012.207-234.

Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49–66. https://doi.org/10.58829/lp.9.2.2022.49-66.

Wilda Hayatun Nufus. "Kejagung Temukan Aliran Kripto Ilegal Bikin Negara Rugi 1,3 Triliun." detiknews, February 6, 2025.

Witold Srokosz, and Tomasz Kopyciaski. "Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability 1." *Journal of Teaching and Education* 04, no. 02 (2015): 619–27. http://www.loc.gov/law/help/bitcoin-.

DECLARATION OF CONFLICTING INTERESTS

The authors states that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

Researcher would like to thank the Directorate of Research and Community Service at the Islamic University of Riau (DPPM-UIR) because the research in this article was fully funded by the Islamic University of Riau through the Internal research scheme of the Islamic University of Riau in 2024.

ACKNOWLEDGMENT

Researcher would like to thank the Faculty of Law at the Islamic University of Riau, INHA Law School, and the Directorate of Research and Community Service at the Islamic University of Riau (DPPM-UIR) who have supported the research in this article with funding sourced from the Islamic University of Riau through the Internal Competitive research scheme at the Islamic University of Riau in 2024.

HISTORY OF ARTICLE

Submitted : March 19, 2025
Revised : March 26, 2025
Accepted : June 2, 2025
Published : June 13, 2025

About Author(s)

David Hardiago, S.H., M.H., is a lecturer, researcher, and Advocate/Legal Consultant affiliated with the Criminal Law Department, Faculty of Law, Islamic University of Riau. Active in conducting research with a focus in the field of Criminal Law, with several publications including: First, self-plagiarism and the principle of legality. Second, Corporations as Subjects in Criminal Acts in the Copyright Sector. Third, Comparative Study of Palgiarism Regulations in the Copyright Law and Criminal Code. The author can be reached via email: davidhardiago23@law.uir.ac.id. For further publications of the author can be accessed through Id Scopus. 58772147500, ID Sinta. 5892960 & https://orcid.org/0000-0002-8350-134X.

Rani Fadhila Syafrinaldi, S.H., M.H., is a lecturer, researcher, and Advocate/Legal Consultant affiliated with the Department of Business Law, Faculty of Law, Islamic University of Riau. Carrying out several research with specifics in the field of Intellectual Property Law (IPR) and its relationship with technology, innovation and business. The author can be reached via email: ranifadhila@law.uir.ac.id For further publications of the author can be accessed via Id Scopus. 59374730200, ID Sinta. 6905741 & https://orcid.org/0009-0002-2189-8377.

Prof. Dr. Syafrinaldi, S.H., M.CL., affiliated with the Postgraduate School of Riau Islamic University, has conducted several research and published articles, some of which are related to this research article, namely: First, Corporations as Subjects in Criminal Acts in the Copyright Sector. Second, Comparative Study of Palgiarism Regulations in Copyright Law and the Criminal Code. Third, Artificial Intelligence in Intellectual Property Law in the Field of Patents. The author can be reached through email: syafrinaldi@law.uir.ac.id For further publiations of the author can be accessed through Id Scopus. 58363300400, Id Sinta. 258281 & https://orcid.org/0000-0002-4064-1756.

Dr. M. Musa, S.H., M.H., is a lecturer and researcher affiliated with the Department of Criminal Law, Faculty of Law, Riau Islamic University. Active in conducting research with the main focus in the field of Criminal Law. The author can be reached via email: musa@law.uir.ac.id For further publications of the author can be accessed via Id Sinta. 6058236 & https://orcid.org/0000-0003-3349-3027.

Kim Hyeonsoo (Prof. Kim Hyeonsoo) which is affiliated with the School of Law Inha University (Seoul – South Korea), has conducted several research and published articles, some of which are related to this research article, namely: First, Public of Criminal Fact in Investigative Agency and Personal Information Protection. Second, Study on Result of Operation in Special Private Security Guard System in Youth Detention Center. Third, A Study on Management System of Gambling Addiction- Focused on Online Gambling Regulation in Australia.