YAYASAN AKRAB PEKANBARU
Akrab Juara : Jurnal Ilmu-ilmu Sosial
Volume 11 Nomor 2 Edisi Mei 2026 (24-33)

4 A LEGAL REVIEW OF THE HANDLING OF MONEY LAUNDERING CRIMINAL ACTS ORIGINATING FROM BITCOIN-BASED INVESTMENT CRIMES

Iqbal Nusantara Al Goni
Universitas Bhayangkara Jakarta Raya
(Naskah diterima: 1 Maret 2026, disetujui: 31 Maret 2026)

Abstract

This study examines the phenomenon of law enforcement against money laundering originating from investment fraud using cryptocurrency (particularly Bitcoin) in Indonesia. In the digital era, the development of information technology has created new investment opportunities through crypto assets, but on the other hand, it has given rise to new financial crime risks such as cyber laundering. The use of virtual currencies has become a preferred method for criminals due to the anonymous and cross-border nature of transactions, making it difficult for authorities to track them. This study uses a descriptive qualitative approach with a library research type. Data sources used include primary legal materials such as Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, as well as secondary legal materials in the form of relevant literature and scientific journals. The results of the study indicate that the law enforcement mechanism against perpetrators of crypto-based money laundering in Indonesia faces significant challenges, both from regulatory aspects that do not specifically regulate the confiscation of digital assets and limited infrastructure and understanding of law enforcement officers regarding blockchain technology. The legal analysis focuses on classifying the perpetrators' actions in the money laundering stages: placement, layering, and integration. It also focuses on how policy formulation, application, and legal execution can be optimized to address evolving modus operandi along with technological advances.
Keywords: *Money Laundering, Crypto Investment, Bitcoin, Cyber Crime.*

Abstract

Penelitian ini mengkaji fenomena penegakan hukum terhadap tindak pidana pencucian uang yang bersumber dari hasil penipuan investasi dengan modus cryptocurrency (khususnya Bitcoin) di Indonesia. Di era digital, perkembangan teknologi informasi telah menciptakan peluang investasi baru melalui aset kripto, namun di sisi lain memunculkan risiko kejahatan keuangan baru seperti cyber laundering. Penggunaan mata uang virtual menjadi modus yang diminati pelaku kejahatan karena sifat transaksinya yang anonim dan lintas batas, sehingga menyulitkan pelacakan oleh otoritas berwenang.Penelitian ini menggunakan metode pendekatan kualitatif deskriptif dengan jenis penelitian kepustakaan (library research). Sumber data yang digunakan meliputi bahan hukum primer seperti Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, serta bahan hukum sekunder berupa literatur dan jurnal ilmiah yang relevan.Hasil penelitian menunjukkan bahwa mekanisme penegakan hukum terhadap pelaku pencucian uang bermodus kripto di Indonesia menghadapi tantangan signifikan, baik dari aspek regulasi yang belum secara spesifik mengatur penyitaan aset digital maupun keterbatasan infrastruktur dan pemahaman

Copyright © 2026 by Author(s)
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

aparat penegak hukum mengenai teknologi blockchain. Analisis yuridis difokuskan pada pengkualifikasian perbuatan pelaku dalam tahapan pencucian uang, yakni placement, layering, dan integration, serta bagaimana kebijakan formulasi, aplikasi, dan eksekusi hukum dapat dioptimalkan untuk mengatasi modus operandi yang terus berkembang seiring kemajuan teknologi.
Kata Kunci: Pencucian Uang, Investasi Crypto, Bitcoin, Kejahatan Siber.

I. INTRODUCTION

In this advanced age, the use of information technology and electronic transactions is absolutely essential because they play a crucial role in supporting the world of trade and accelerating national economic growth (Abdul Halim Barkatullah, 2017). Various new electronic currencies, including cryptocurrency, are emerging. Money laundering through virtual currency (Bitcoin) is a new method that can be used by individuals to launder proceeds of crime. This money laundering method leverages technological advances in the cyber sector. Also known as cyber laundering, it is the use of internet-based electronic transfer methods to disguise the source of illegal funds. This type of crime occurs due to the emergence of virtual currencies that have spread to various global payment networks and the internet, including electronic payment systems and internet banking systems. (Amrani, Hanafi, 2010)

Cryptocurrency offers ease of transactions and high profit potential, but it also carries significant risks, particularly related to fraud and money laundering. Investment fraud through cryptocurrency has become a rapidly growing phenomenon, with perpetrators seeking to exploit the public's ignorance and tendency to invest in digital assets perceived as promising. Cryptocurrency, based on blockchain technology, offers security and transparency in transactions. However, these characteristics also make them vulnerable to abuse. Cryptocurrency investment scams often involve seemingly legitimate schemes, where the perpetrators offer investments with highly attractive rewards. Typical modus operandi include Ponzi schemes: where the perpetrator promises high returns to early investors by using funds from new investors, creating the illusion of profit; Phishing: where the perpetrator uses manipulation techniques to gain access to victims' digital wallets; and Disguising as an Investment Platform: where the perpetrator creates a website or app that looks like a legitimate investment platform to deceive potential investors. When victims are defrauded and lose their money, the perpetrators often launder money to conceal the proceeds of their crimes, making it extremely difficult to trace the funds. Money laundering is the process used to conceal the origins of funds obtained through illegal activities. In general, money laundering involves three stages: Placement: Inserting the proceeds of crime into the financial system, often through

bank deposits or asset purchases, Layering: Carrying out a series of transactions to hide the trail of funds, such as transferring funds between accounts or investing in liquid assets, Integration: Taking the cleaned funds and using them in legitimate economic activities.

Therefore, in the context of cryptocurrency, money laundering can be carried out in more complex and difficult-to-trace ways, thanks to the decentralized nature and anonymity offered by many cryptocurrency platforms. The modus operandi used includes various forms of opaque investment offers, quick money-doubling schemes, and Ponzi schemes. After successfully raising funds from investors, perpetrators often launder money to conceal their crimes and divert the funds into more difficult-to-trace assets. Law enforcement against perpetrators of money laundering crimes originating from cryptocurrency investment fraud is crucial to protect the public and maintain economic stability.

However, law enforcement in this context faces several challenges, such as the lack of clear regulations, the difficulty in tracing digital transactions, and the complexity of the technology used by perpetrators. Furthermore, the large number of jurisdictions involved in cryptocurrency transactions complicates coordination between law enforcement agencies across countries. Indonesia, as one of the countries with the fastest-growing cryptocurrency user base, needs a comprehensive approach to addressing this issue. Effective law enforcement will not only minimize the opportunities for perpetrators to commit money laundering but will also increase public trust in digital investment and financial systems. Therefore, it is necessary to conduct an in-depth study of the strategies, regulations, and challenges faced in law enforcement against perpetrators of money laundering crimes from cryptocurrency investment fraud, in order to formulate appropriate and effective solutions.

II. RESEARCH METHODS

This research uses a normative legal research method with two main approaches: a conceptual approach and a statutory approach. This combination is applied to produce a prescriptive analysis, namely providing constructive legal recommendations.

III. RESEARCH RESULTS

A. Forms of money laundering crimes from cryptocurrency investment fraud, especially Bitcoin.

Money Laundering (TPPU) in cryptocurrency investments like Bitcoin is a double crime that is always preceded by a predicate crime, such as fraud. According to Article 1 of Law Number 8 of 2010, proceeds of crime include wealth from corruption, fraud, and other crimes,

which carry a minimum prison sentence of four years. Although it has been criminalized globally in accordance with international recommendations, TPPU lacks a standard, universal definition due to differences in policy focus between countries. In Indonesia, the main challenge arises from the anonymous and cross-border nature of Bitcoin, but regulations still categorize any attempt to conceal the origin of funds from illegal investments as a form of money laundering, which is punishable by law.

1. Forms of Qualification for Money Laundering Crimes.

The characteristics of TPPU make TPPU a double crime. This means that the emergence of TPPU is always preceded by the original crime.19 The TPPU Law itself determines the types of crimes that are the source of wealth whose origins are then disguised as regulated in Article 1 of Law Number 8 of 2010, namely: The results of criminal acts are assets obtained from criminal acts of corruption, bribery, narcotics, psychotropics, labor smuggling, migrant smuggling, banking, capital markets, insurance, customs, excise, human trafficking, illegal arms trafficking, terrorism, kidnapping, theft, embezzlement, fraud, counterfeiting, gambling, prostitution, taxation, forestry, environmental, maritime and fisheries, other crimes that are threatened with imprisonment of 4 (four) years or more, which are committed in the territory of the Unitary State of the Republic of Indonesia or outside the territory of the Unitary State of the Republic of Indonesia and the crime is also a crime according to Indonesian law and assets that are known or reasonably suspected to be used and/or used directly or indirectly for terrorist activities, terrorist organizations, or individual terrorists are equated with the proceeds of criminal acts as referred to in paragraph (1) letter n. Although the Crime of Money Laundering (TPPU) has been recognized as a crime by the international community and various countries have committed to criminalizing money laundering, TPPU itself does not yet have a standard and universal definition across countries. Differences in background and focus in the preparation of criminal policies for the crime of money laundering in various countries are the cause. For example, England and France use money laundering instruments as part of drug eradication efforts. (Budi Saiful Haris, 2016). Meanwhile, in America, the goal is to combat crime more broadly, not limited to narcotics alone. In Indonesia, referring to the Law on the Crime of Money Laundering, the definition of the Crime of Money Laundering is not explicitly stated. This can be seen in the first regulation of money laundering in Indonesia, namely Law Number 15 of 2002 concerning the Crime of Money Laundering in conjunction with Law Number 23 of 2003 concerning Amendments to Law Number 15 of 2002 concerning the Crime of Money Laundering only defines money laundering through the form of the offense, namely:

Article 1 In this Law, what is meant by: "Money Laundering is the act of placing, transferring, paying, spending, granting, donating, depositing, taking abroad, exchanging, or other actions regarding Assets that are known or reasonably suspected to be the result of a crime with the intention of hiding or disguising the origin of the Assets so that they appear to be legitimate Assets." The latest Money Laundering Law, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (AML) only defines Money Laundering as follows: Article 1 In this law, "Money Laundering" means any act that fulfills the elements of a crime in accordance with the provisions of this law. Unlike the United States, which has a very broad scope of crime prevention, Indonesia does not define Money Laundering (AML) explicitly in one standard sentence, but rather through a description of the form of the offense. In Law No. 15 of 2002, AML is explained as an effort to place or disguise the proceeds of crime so that they appear legitimate, while Law No. 8 of 2010 further simplifies the definition as any act that fulfills the elements of a crime according to the articles therein (especially Articles 3, 4, 5, and 6). This element-based approach to criminal acts was chosen to make Indonesian law more flexible and adaptable in accommodating the modus operandi. an operation that continues to develop along with technological advances, without eliminating its basic philosophy, namely severing the link between illegal assets and their original source.

2. Money laundering crimes related to cryptocurrency investment fraud, especially Bitcoin.

Crypto is a digital asset whose value is determined by the market, much like stocks or bonds, and can be traded on various crypto exchanges such as INDODAX. Digital assets, which use cryptography for security, operate independently of central banks. Unlike traditional currencies, crypto utilizes blockchain technology to record and verify transactions in a decentralized manner. This concept is revolutionary in the financial world because it eliminates the need for trusted third parties like banks in financial transactions. Instead, crypto relies on a distributed network of computers running open-source software to validate and record each transaction. Crypto assets use cryptography and blockchain technology to ensure security, transparency, and prevent counterfeiting through a distributed ledger system. While its fundamentally decentralized nature frees crypto from the control of a central authority, it also poses the risk of high volatility and misuse for illegal activities such as money laundering through placement, layering, and integration mechanisms. In Indonesia, crypto assets such as Bitcoin are only recognized as commodities supervised by Bappebti and are strictly prohibited as a means of payment because it is contrary to Law Number 7 of 2011. Law enforcement

against misuse of these assets refers to Law Number 8 of 2010, which ensnares perpetrators for controlling assets known or reasonably suspected to originate from criminal acts, in order to prevent Indonesia from becoming a hotbed of crime that can damage its international image.

B. Law enforcement mechanisms in Indonesia against perpetrators of money laundering originating from cryptocurrency investments.

This process begins with an investigation into predicate crimes (such as investment fraud), which is then combined with a money laundering (TPPU) investigation if evidence of asset transfer to digital form is found. Law enforcement officials, such as the Indonesian National Police (Polri) and prosecutors, collaborate with the Financial Transaction Reports and Analysis Center (PPATK) to trace the flow of funds from suspicious transactions and coordinate with the Commodity Futures Trading Regulatory Agency (Bappebti) to monitor registered crypto asset traders. Enforcement is carried out by freezing accounts on local exchange platforms and seizing assets through private key acquisition or transferring balances to state-owned digital wallets as evidence in court. However, the effectiveness of this mechanism is hampered by the decentralized and anonymous nature of crypto assets, making it difficult to implement traditional audit trails. The main obstacle lies in regulatory gaps, where the TPPU Law does not explicitly define crypto assets, but only covers approximate phrases such as "e-money organizers." Furthermore, the reverse burden of proof procedure under Articles 77 and 78 is often technically difficult to enforce in court due to the lack of specific operational regulations regarding virtual assets. As a result, law enforcement is often only effective if the perpetrator interacts with formal financial institutions within the country, while transactions that occur entirely on foreign exchanges or through private wallets remain an area that is difficult to reach legally.

1. Modus Operandi of Money Laundering Crimes Originating from Cryptocurrency Investments.

Money laundering through digital assets like Bitcoin is a new modus operandi for disguising and exploiting the proceeds of crime, both in the real and virtual worlds. Although popular among investors, cryptocurrencies are often misused by criminals to launder funds from digital fraud and theft of online exchange assets. In Indonesia, Bitcoin is only recognized as a commodity that can be traded on futures exchanges under the supervision of Bappebti (Commodity Futures Trading Regulatory Agency), but its use as a means of payment is strictly prohibited as it violates Law No. 7 of 2011 concerning the mandatory use of the Rupiah currency. This virtual money laundering can be further explained as follows:

a. Layering (Transfer): This process aims to cut off the trail of wealth from its source, making it difficult to trace. Cryptocurrency has become a popular means due to its anonymity, lack of central control, and automation. In Indonesia, law enforcement (such as confiscation of crypto assets) is hampered by the lack of specific regulations, the lack of adequate internet infrastructure, and limited knowledge of blockchain technology by law enforcement.

b. Placement: This stage involves transferring the proceeds of crime into the formal financial system. Based on Law No. Law No. 8 of 2010 requires financial service providers to report suspicious transactions, cash transactions exceeding IDR 500 million, or overseas transfers to the Financial Transaction Reports and Analysis Center (PPATK). However, this regulation does not yet cover cryptocurrency operators. This legal loophole exists because the nature of cryptocurrency (virtual money without a physical form) differs from e-money or e-wallets, as regulated by current regulations, leaving its users vulnerable to legal action.

c. Integration: The final stage involves transferring the "laundered" wealth into legitimate economic activities to allay suspicion. Perpetrators typically purchase luxury goods, property, or establish companies. This practice is often carried out in countries with weak money laundering regulations, ultimately damaging the country's international image.

Money laundering using fiat currency is easier to track because it is centralized under the banking system and supported by Law No. 8 of 2010. In contrast, money laundering through crypto assets is difficult to detect because it is decentralized, anonymous, and does not require the intervention of financial institutions, thus breaking the audit trail. Cryptocurrency trading utilizes the concept of reverse layering, whereby fiat currency is converted into digital assets to disguise its true form. To date, Indonesian regulations have not specifically addressed cryptoeconomic actors; the term "e-money provider" in the law cannot be equated with cryptocurrency due to fundamental differences in physical form and storage mechanisms.

2. Legal Analysis of Money Laundering Enforcement from the Proceeds of Cryptocurrency Investment Fraud.

Criminal law enforcement is an integrated process aimed at achieving justice, legal certainty, and social benefits. However, in the context of money laundering (TPPU), legal uncertainty exists because the Corruption Eradication Commission (KPK) only has the authority to investigate concurrently with the predicate offense (as stipulated in Articles 74 and 75 of Law No. 8 of 2010), but lacks the authority to prosecute. Therefore, prosecution must be delegated to the Prosecutor's Office. Materially, money laundering (TPPU) involves the perpetrator through elements of intent or negligence (culpa), but current regulations do not

clearly define the procedures and technical consequences of the reverse burden of proof system. To limit the scope of criminal activity for perpetrators, such as corruptors, Indonesia has adopted the FATF recommendation by criminalizing various proceeds of crime, which are subject to imprisonment of four years or more, as objects of money laundering.

The implication of this legal situation is the creation of bureaucratic inefficiencies due to the separation of investigative authority at the KPK and prosecution at the Prosecutor's Office, which has the potential to delay legal certainty for defendants. Furthermore, the application of the negligence element (culpa) imposes a high legal burden on both the public and financial service providers, as ignorance perceived as negligence can lead to criminal prosecution. Technically, the lack of standard procedures for the reverse burden of proof creates uncertainty regarding asset execution, where judges may hesitate to issue confiscation orders if the defendant's defense mechanisms are not clearly defined. However, on the other hand, expanding the scope of predicate crimes in accordance with international standards strengthens the state's reach to pursue the proceeds of crime in various new sectors, including digital investment.

IV. CONCLUSION

Based on the research and discussion, the following conclusions can be drawn:

First, the form of money laundering from cryptocurrency investment fraud, particularly Bitcoin, is regulated in the Money Laundering Law to determine the various types of crimes that result in the source of assets that are then disguised, as stipulated in Article 2 Paragraph (1) letter r of Law Number 8 of 2010. Money from cryptocurrency investment fraud, particularly Bitcoin, is often processed through several stages aimed at concealing the origin of the illicit funds. Fraudsters typically attract investors with promises of unrealistic returns, then use money laundering techniques such as layered transactions, the use of anonymous wallets, and poorly supervised exchange platforms to obscure the trail of their illegally obtained funds.

Second, law enforcement against perpetrators of money laundering from cryptocurrency investment fraud, such as Bitcoin, is generally no different from handling other criminal cases. However, handling money laundering cases involves a relatively new institution, the Financial Transaction Reports and Analysis Center (PPATK). After receiving the analysis results from the PPATK, police investigators then conduct an investigation. The investigation and investigation of money laundering crimes are based on the Criminal Procedure Code (KUHAP).

REFERENCES

Abdul Halim Barkatullah, 2017, Electronic Transaction Law in Indonesia, Nusa Media, Bandung.

Abdurrahmat Sathoni, 2005. Research Methods and Thesis Writing Techniques, RinekaCipta, Jakarta.

Adrian Sutedi, 2008, The Crime of Money Laundering, PT Citra Aditya Bakti, Bandung.

Ahmad Rifai, 2010, Legal Discovery by Judges, From a Progressive Legal Perspective, Sinar Grafika, Jakarta.

Amiruddin and H. Zainal Asikin, 2012, Introduction to Legal Research Methods, Sixth Edition, PT Rajagrafindo Persada, Jakarta.

Amrani, Hanafi. 2010. Criminal Law on Money Laundering. Yogyakarta: UII Press. Andi Hamzah, 1994, Problems of Criminal Law Enforcement, Jakarta.

Axel Yohandi, et al., 2024, "Legal Implications of Using the Virtual Currency Bitcoin as a Means of Payment in Commercial Transactions (A Comparative Study Between Indonesia and Singapore)"

Bambang Purnomo, 2011, "Money Laundering: Perceptions of Socio-Economic Law with Criminal Aspects," PT Raja Grafindo Persada, Jakarta.

Budi Saiful Haris, "Strengthening Evidence of Money Laundering in Corruption Cases in Indonesia," Jurnal Integritas, Volume 02 Number 1, 2016.

Commodity Futures Trading Supervisory Agency Regulation Number 7 of 2020 concerning the Determination of the List of Crypto Assets That Can Be Traded on the Physical Crypto Asset Market.Abdul Halim Barkatullah, 2017, Hukum Transaksi Elektronik Di Indonesia, Nusa Media, Bandung.

Gayung Utami, "Legal Analysis of the Use of Cryptocurrency (Bitcoin) as a Means of Money Laundering," Volume 01 Number 01, 2012.

Hans Kelsen, "Pure Legal Theory," Foundations of Normative Legal Science, Second Edition, Translated from Hans Kelsen's book, "Pure Theory of Law" (Berkeley: University of California Press, 1978), (Bandung: Publisher Nusamedia and Publisher Nuansa, 2007).

Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU).

Law Number 30 of 2002 concerning the Corruption Eradication Commission (KPK).

Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE).Made Pasek Diantha, 2016. Normative Legal Research Methodology in the Justification of Legal Theory. Jakarta: Kencana.

Novia Imam N & Mohammad Djasul, "Legal Analysis of Money Laundering Crimes from an Islamic Law Perspective," Volume 2, Number 1, 2023.

Peter Mahmud, Marzuki. 2012. Introduction to Legal Science. Jakarta: Kencana Prenada.

OCBC NISP Editorial Team, "What is Cryptocurrency? "How It Works, Types, & Risks," Website, October 2, 2023.

Rifki Adhyaksa Mahendra, "Modus Operandi of Money Laundering Through Virtual Money (Cryptocurrency): A Positive Law and Islamic Criminal Law Perspective (Case Study of PT. Asabri)," Surakarta, September 26, 2023.

R. Wiyono, 2014, "Discussion of the Law on the Prevention and Eradication of Money Laundering," Sinar Grafika, Jakarta.

Soerjono Soekanto and Sri Mamudji, 1985, "Research on Normative Law: A Brief Review," CV. Rajawali, Jakarta.

Suhartoyo, 2018, "Argument for Reversing the Burden of Proof as a Priority Method in Eradicating Corruption and Criminal Acts" Money Laundering, PT Raja Grafindo Persada, Jakarta.