Journal of Social Research

P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

Reform of Law Enforcement to Strengthen the Legal System in Eradicating Money Laundering Through Cryptocurrency Investments

Rusman[1], Zudan Arief Fakrulloh[2]

Universitas Borobudur, Indonesia[1, 2]

Email: *kompolrusman72@gmail.com[1], cclsis@yahoo.com[2]*

ABSTRACT

Cryptocurrency investments are rapidly developing worldwide, including in Indonesia. Behind its profit potential, digital assets also open opportunities for criminals to commit money laundering offenses. The anonymity, pseudonymity, and decentralization of blockchain technology underlying cryptocurrencies create challenges for law enforcement in tracking illegal activities that exploit these assets. This study aims to examine the role of existing regulations in preventing the use of digital assets as a means of money laundering and to identify the challenges faced by law enforcement in enforcing rules against suspected cryptocurrency transactions. The research will analyze the extent to which the existing regulations, both at the national and international levels, are effective in preventing the use of cryptocurrencies for money laundering crimes. The second subtitle will explore various technical and legal constraints faced by law enforcement, including the lack of international cooperation, limitations of monitoring technology, and the low level of technical expertise among law enforcement officials.

Keywords: *Cryptocurrency Investment, Money Laundering, Law Enforcement, Legal Reform.*

INTRODUCTION

The development of financial technology has reached a stage where its services and operations are no longer limited by geographical areas and have surpassed various jurisdictions, a phenomenon often referred to as economic globalization. For example, financial technology services provide facilities such as the use of credit and debit cards accepted in almost all countries, investment in virtual assets, and payment execution via electronic money and mobile devices. Entering the era of the Fourth Industrial Revolution and moving towards Society 5.0, there has been a transformation in financial transactions from initially being conducted offline to online, a term known as financial technology or fintech. The development of payment transactions has evolved from cash-based instruments to non-cash-based instruments, further advanced with paperless transactions. Additionally, the current phenomenon being widely discussed in Indonesian society is the emergence of cryptocurrency (Group, 2022).

The advancement of financial technology and economic globalization has a positive impact on the development of the financial, economic, and business sectors. However, alongside the proliferation of organized non-conventional crimes, money laundering offenses have emerged as one of the most dominant and prevalent forms of crime compared to other types of non-conventional crimes. Therefore, along with the development of financial technology and economic globalization—which has resulted in increased cross-border crime—cryptocurrencies, as a product of technological advancement, are now a public concern. In Indonesia, cryptocurrencies are currently not viewed as currency because they are not issued by an authorized authority, such as Bank Indonesia. However, in various countries such as the Netherlands, the United Kingdom, Germany, Japan, the United States, and Switzerland, cryptocurrencies have been recognized and legitimized as currency, with policies designed to prevent their misuse, particularly concerning money laundering offenses (Indonesia, 2008).

Cryptocurrencies are a form of digital asset that utilizes blockchain technology (distributed ledger) and cryptography. These assets are characterized by high price volatility, making them unable to optimally perform the three functions of money: as a store of value, a medium of exchange, and a unit of account. Within cryptocurrency, there are also stablecoins introduced to protect the value of investment from existing volatility. Juridically, cryptocurrencies are understood as digital assets categorized as intangible commodities, where the processes of transaction verification and security do not involve third parties. In Indonesian law, the term "Cryptocurrency" is referred to as "Crypto Asset," as explained in Article 1 point (7) of the Regulation of the Commodity Futures Trading Regulatory Agency Number 5 of 2019 on Technical Provisions for the Implementation of the Physical Crypto Asset Market. Cryptocurrency is defined as an intangible commodity in digital form that utilizes cryptography, peer-to-peer networks, and distributed ledgers to regulate the creation of new units, verify transactions, and secure transactions without involving third parties. Furthermore, the term cryptocurrency is also referred to as "virtual currency" in the explanation of Article 34 letter a of Bank Indonesia Regulation Number 18/40/PBI/2016 on Transaction Processing, which refers to money issued by parties other than monetary authorities, acquired through mining processes, purchases, or transfer rewards, including Bitcoin, BlackCoin, Dash, Dogecoin, Litecoin, Namecoin, Nxt, Peercoin, Primecoin, Ripple, and Ven.

Currently, in Indonesia, there is a significant risk associated with the use of cryptocurrencies as instruments in the execution of money laundering offenses. Money laundering is a major issue faced by governments and institutions worldwide, as it has a negative impact on institutional integrity and the economy. Money laundering can be defined as efforts to conceal the origins of money obtained illegally. This practice is often related to activities such as corruption, bribery, terrorism, and the trafficking of arms and drugs. However, there are also other actions rarely highlighted, such as human trafficking, tax evasion by individuals or companies, and illegal fuel sales, which also often occur within the context of money laundering (Kurniawan, 2012).

Funds obtained from illegal activities are typically spent in cash or directly deposited into the financial system. When the amount involved is relatively small, money launderers tend to make cash purchases in small amounts without using financial intermediaries. This means that the cash can be used to buy items like food and equipment or transferred to other parties for peer-to-peer debt payment, thereby automatically laundering the money. Conversely, when the amounts involved are substantial, money launderers typically deposit the funds into the financial system to exploit existing vulnerabilities. Once the money is in the financial system, it undergoes a complex process to be laundered.

The key stages in the money laundering process within the financial system include placement, layering, and integration. Conventional methods used to detect money laundering activity involve applying rule-based systems that establish characteristics of suspicious transactions. The primary weakness of this method lies in the high rate of false positives and wasted investigation costs, as this system is static and less capable of adapting to changing crime patterns. However, with technological advancements, artificial intelligence techniques are starting to be implemented to overcome the limitations of traditional detection methods. During layering and integration, money laundering perpetrators attempt to obscure their illegal funding sources. At the same time, the funds that have entered the financial system are also at risk from other crimes, such as cybercrime (Rohman, 2021). Cybercriminals can hack into savings or debit accounts and transfer stolen money to other accounts to gain full control over those funds. Hacking activities are illegal actions performed in cyberspace, supported by modern technology that enables criminals to steal personal data and access information on accounts.

Once the funds are stolen, they can be distributed to various accounts, both in national and international banks, to further layer within the financial system, making the origin of the illegal funds increasingly difficult to trace. Subsequently, these funds are integrated into legitimate activities through electronic transactions, such as payments for purchasing vehicles or houses, credit loan repayments, mutual fund purchases, or binding insurance contracts and private pension programs. This example illustrates a money laundering process fully operating in the digital realm, from fund acquisition, placement, layering, to integration. Based on the explanations provided, the regulation of money laundering offenses (TPPU) still faces challenges due to a lack of clear regulations. Therefore, this research will discuss the role of current cryptocurrency regulations in preventing the use of digital assets as a means of money laundering, whether these regulations are sufficient, and what challenges law enforcement faces in monitoring and enforcing the law against cryptocurrency transactions suspected of involvement in money laundering (Handa & Ansari, 2022).

METHOD

In this study, the legal research methodology, also known as the statue approach or normative legal research, is a process of finding legal rules, principles, and legal doctrines to address legal issues. This approach is used to ascertain the role of current cryptocurrency regulations in preventing the use of digital assets as a means of money laundering, whether these regulations are sufficient, and the legal gaps that govern cryptocurrency investments. The case approach is also employed to analyze and study relevant legal problems to identify the gaps and challenges faced by law enforcement in monitoring and enforcing the law against cryptocurrency transactions suspected of involvement in money laundering. Additionally, a conceptual approach is taken, rooted in the views and doctrinaire perspectives of legal scholars that have developed in the field of law.

RESULTS AND DISCUSSION

The Role of Cryptocurrency Regulation in Preventing the Use of Digital Assets as a Means of Money Laundering

Cryptocurrency has two primary functions: as a medium of exchange and as a commodity. In its capacity as a medium of exchange, cryptocurrency possesses characteristics resembling currency, as it can be used as a payment instrument in certain situations, and its value remains relatively stable given the limited amount of its issuance. However, cryptocurrencies were initially not recognized as legitimate and official means of payment because there is no authority responsible for issuing, regulating, managing circulation, and maintaining the stability of its value. These functions are wholly operated by computational systems, raising concerns regarding accountability (Rani et al., 2021).

From a legal perspective in Indonesia, cryptocurrency is not recognized as a legitimate means of payment, as it does not meet the provisions of applicable legislation. According to Article 23B of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) in conjunction with Article 1 points 1 and 2, Article 2 paragraph (1), and Article 21 paragraph (1) of Law Number 7 of 2011 concerning Currency (Law No. 7/2011), the legitimate money is the means of payment officially authorized by the state and the government. Article 21 of Law No. 7 of 2011 stipulates that the only legally recognized means of payment within the territory of Indonesia is the rupiah, which is officially issued by Bank Indonesia. Furthermore, Article 21 of Law No. 7 of 2011 mandates the use of rupiah in:

(a) every transaction intended to make a payment;
(b) the fulfillment of other obligations that must be settled with money; and/or
(c) other financial transactions conducted within the territory of the Unitary State of the Republic of Indonesia.

Digital Rupiah is essentially a form of virtual asset or digital asset. According to the definition of virtual assets by the Financial Action Task Force (FATF), a virtual asset is a digital representation of value that can be traded or transferred digitally and can be used for payment or investment purposes. Referring to this definition, Digital Rupiah meets two criteria that classify it as a virtual asset: first, as a digital representation of the value of the rupiah currency, and second, its ability to be transferred digitally as a means of payment. As a virtual asset, Digital Rupiah also presents both opportunities and challenges, particularly concerning the risks of its misuse as a new medium for money laundering, terrorism financing, and other crimes. This risk stems from the capability and ease that Digital Rupiah possesses in conducting fast cross-border transactions, which not only allows criminals to obtain, transfer, and store assets digitally, often outside the regulated financial system, but also complicates tracking the source or destination of funds and hinders reporting entities in identifying suspicious activities in a timely manner (Pudjastuti & Westra, 2021). Therefore, before Digital Rupiah is widely adopted, policy reforms regarding money laundering in Indonesia are necessary to anticipate potential risks that may arise.

The regulation of the Commodity Futures Trading Regulatory Agency (BAPPEBTI) No. 7 of 2020 establishes a list of cryptocurrencies that can be traded in the physical cryptocurrency market. The main reason why cryptocurrency is difficult to classify as a legitimate national currency, particularly in Indonesia, is that the price fluctuations of digital currencies are not influenced by national policies or economic conditions. The value of each cryptocurrency is determined based on the supply and demand mechanisms of users, much like the prices of ordinary commodities, making their value unstable and difficult to maintain. This contrasts with fiat money, which has been widely accepted by society and can be used by anyone, while cryptocurrency only exists in the virtual realm and can only be used by users involved in that ecosystem (Firdaus, 2023). Based on this, the steps that the government can take are to formulate clear regulations regarding cryptocurrency, considering the trends of cryptocurrency use at a global level. The use of cryptocurrency is also influenced by the need for improvements in the existing monetary system. Therefore, in formulating regulations on cryptocurrency, the government needs to address the following matters:

1. The legal status of cryptocurrency, whether it is recognized as currency or only as a medium of exchange.
2. Restrictions related to the place and use of cryptocurrency.
3. Oversight of transaction flows involving cryptocurrency.
4. Imposition of taxes on cryptocurrency transactions.
5. Provision of deposit guarantees for cryptocurrency users.
6. Assimilation of blockchain systems and concepts in the management of currency.

It is important to note that there are several factors that make cryptocurrencies significantly attractive to investors. First, these currencies are independent as they are not regulated or supervised by any central authority. Second, the flexibility of transactions is very high, as they can be conducted anytime and by anyone directly, with remarkable speed and relatively low costs. Third, cryptocurrency transactions are very secure because they utilize layered encryption technology, making it nearly impossible to hack or trace. The more honest users there are, the stronger the security system becomes (Puspasari, 2019). Fourth, for merchants who accept cryptocurrencies, the transaction risks are lower because the transactions are final and cannot be reversed, unlike credit or debit card transactions that can fail for various reasons, such as exceeding credit limits, insufficient balance, or cancellations by issuing banks. Fifth, the presence of merchants and cryptocurrency exchanges allows this digital currency to be easily converted into other official currencies.

However, transactions with cryptocurrencies have anonymous characteristics, where users do not need to disclose their identities or use pseudonyms, making it difficult to trace those transactions. This leads to a high potential risk for cryptocurrencies to be utilized in illegal transactions. Authorities in the United States have found evidence that cryptocurrencies are used by various parties for illegal activities, such as arms trading, selling hacking software for websites, and drug transactions. Additionally, cryptocurrencies have several weaknesses, particularly due to their lack of recognition as legitimate and official currency. These assets are not issued by any authorized authority, such as Bank Indonesia, which has the authority to issue, regulate, manage the circulation and distribution of currency, as well as guaranteed authenticity and maintain exchange rate stability (Almeida et al., 2023). In the scheme of cryptocurrencies, all these functions are carried out by computational systems, leaving no clear party responsible for their issuance and management. Meanwhile, several criteria must be met for an object to be deemed suitable as a medium of exchange or payment tool: (i) Acceptability, the item must be widely accepted by the public; (ii) Durability, the item used as a payment method must be durable and not easily damaged; (iii) Scarcity, the item must have uniform quality, be available in sufficient quantities to meet public demand, and be difficult to counterfeit; and (iv) Stability, the item must be easy to transport, easy to divide without losing value, and have maintained value stability.

Oversight of cryptocurrency misuse needs to be heightened due to the high potential for these assets to be used by perpetrators to conceal the proceeds of money laundering crimes. Cryptocurrencies also create negative impacts because their characteristics hinder law enforcement agencies in tracking and monitoring, providing advantages to criminals in their efforts to hide the proceeds of illegal activities. The lack of legal regulations regarding cryptocurrency usage results in weak oversight on money laundering using cryptocurrency (Lin et al., 2024). Two important elements in combating money laundering in the crypto industry are the Anti-Money Laundering (AML) Guidelines 5 and the Markets in Crypto-Assets (MICA) law. For example, the UK has begun to draft its own regulatory framework for crypto. In addition to establishing clear rules for actors involved in crypto transactions, the European Union and the UK have also designed rules and principles to protect against the misuse of crypto assets. These steps aim to create a safer and more transparent environment for all players in the crypto industry. However, many crypto operators choose not to comply with regulations and continue to operate without Anti-Money Laundering (AML) measures. Criminals, both in the traditional financial sector and in crypto, often seek platforms that lack adequate AML mechanisms to conduct their illegal activities. Although some crypto platforms comply with AML standards, there are still users who can bypass those controls (Weber et al., 2019).

The money laundering process involving cryptocurrencies typically goes through several stages, including Layering, which is the process of severing the connection between assets and their sources to disguise the origin of funds and complicate tracking. Cryptocurrency transactions are anonymous and regulated automatically by electronic systems without central authority oversight, making them an ideal means to hide illegal funds. The next stage is Placement, where illegally obtained wealth is inserted into the financial system through banks or other financial institutions (Wu et al., 2023). Finally, Integration is the stage where proceeds from crime are invested in legitimate economic activities, such as purchasing luxury goods, real estate, or other assets, with the aim of eliminating suspicion from law enforcement officials. One example of a case involving money laundering with cryptocurrency occurred in 2023, when Rafael Alun was prosecuted, and based on the appeal decision No. 75/Pid.Sus-TPK/2023/PN Jkt Pst issued on January 8, 2024, the Corruption Crime Court at the Central Jakarta District Court stated that he was found guilty of committing corrupt acts with the following charges:

1. First Charge: Article 12B in conjunction with Article 18 of the Republic of Indonesia Law Number 31 of 1999 on the Eradication of Corruption Crimes, as amended by the Republic of Indonesia Law Number 20 of 2001, in conjunction with Article 55 paragraph (1) subparagraph 1 of the Indonesian Penal Code (KUHP) and Article 64 paragraph (1) of the KUHP.
2. Second Charge: Article 3 paragraph (1) letters a and c of the Republic of Indonesia Law Number 15 of 2002 on Money Laundering Crimes, as amended by the Republic of Indonesia Law Number 25 of 2003, in conjunction with Article 55 paragraph (1) subparagraph 1 of the KUHP and Article 64 paragraph (1) of the KUHP.
3. Third Charge: Article 3 of the Republic of Indonesia Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes, in conjunction with Article 55 paragraph (1) subparagraph 1 of the KUHP and Article 64 paragraph (1) of the KUHP.

In this case, Rafael has committed money laundering by diverting the proceeds from bribery into cryptocurrency assets. Evidence of this was found during the tracing of the cryptocurrency assets, by examining the statement of accounts belonging to Rafael. During the tracing process, the Head of the Financial Transaction Reports and Analysis Center (PPATK), Ivan Yustiavandana, stated that his agency found transactions related to Rafael's ownership of bitcoin, as Rafael Alun's e-wallet was also one of those monitored by PPATK. This was because the e-wallet had previously been involved as a means of Money Laundering Crime (TPPU) in several other cases. In the tracing of cryptocurrency transactions, PPATK used this data as a basis for their analysis. In some cases, they handled PPATK even went so far as to freeze the e-wallet of the TPPU suspects.

The e-wallet, also known as a digital wallet, is a platform service based on applications that facilitates users in storing money and using it as a payment method. The e-wallet functions as electronic evidence in Rafael's case, where this e-wallet falls under the category of electronic information according to Article 1 number 1 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions. This electronic information includes one or a collection of electronic data, including but not limited to writings, sounds, images, maps, designs, photos, electronic data interchange (EDI), emails, telegrams, telexes, telecopies, or similar items that have been processed and hold meaning or can be understood by competent parties.

In this case example, money laundering can be defined as any act carried out with the aim of frustrating the identification of the origin, tracing, or seizure of assets known or suspected to be derived from criminal acts. Meanwhile, it defines money laundering as the attempt to convert assets obtained illegally into assets that appear to be legitimate by mixing them with lawful money, thus making it very difficult to distinguish between what is legitimate money and what is not. Based on these doctrinal considerations, it can be concluded that money laundering has two main meanings:

(a) (a) obstructing or complicating the identification of the origin, tracing, or seizure of assets, which is known as the act of hiding;

(b) making the proceeds of crime appear as legitimate assets, which is referred to as the act of disguising. Thus, the essence of money laundering lies in the effort to hide or disguise the origin of the proceeds from criminal acts.

Regarding the weaknesses of cryptocurrency regulations in Indonesia in preventing the use of digital assets as a means for money laundering, the main issues lie in the lack of understanding and adaptation to the unique characteristics of digital assets. Although the Commodity Futures Trading Regulatory Agency (Bappebti) has begun to regulate cryptocurrency trading through regulations that set rules for crypto platforms, these regulations are often seen as less comprehensive in terms of transparency and oversight.

One of the main weaknesses is the lack of an effective monitoring system for cryptocurrency transactions, which are often pseudonymous and decentralized. As a result, individuals intending to engage in money laundering can exploit this gap to obscure the source and purpose of their funds. Additionally, limitations in the implementation of Know Your Customer (KYC) and Anti-Money Laundering (AML) technologies on several cryptocurrency platforms in Indonesia also pose a problem. Although regulations for KYC and AML have been established, their implementation remains inconsistent, especially on smaller or newly developed platforms. This opens opportunities for financial criminals to take advantage of system weaknesses, conduct transactions anonymously, and transfer funds across regions without detection.

The absence of integrated global regulations also poses a challenge, as money laundering activities can easily involve cross-border transactions, while local authorities have limited capacity to monitor international transactions. Enforcement of laws remains weak in addressing digital financial crimes in Indonesia, which complicates efforts to prevent money laundering through digital assets. Law enforcement often faces technical obstacles in tracing and understanding the complex flow of cryptocurrency transactions, particularly due to limited digital infrastructure and expertise in analyzing blockchain data.

Thus, without improvements in regulations, monitoring technology, and better international coordination, cryptocurrencies are likely to continue being an attractive tool for money laundering actors.

Legal Vacuum in Cryptocurrency Transactions Suspected of Involvement in Money Laundering

Looking at regulations in the United States and Japan, there are several aspects of the cryptocurrency ecosystem that have not been specifically regulated by the Indonesian government but are addressed in the U.S. and Japan. One of these aspects involves Non-Fungible Tokens (NFTs), which are unique digital assets that cannot be directly exchanged for other tokens. Additionally, regulations regarding Stablecoins—cryptocurrencies whose value is pegged or supported by fiat currency—have not yet received clear regulatory attention in Indonesia. The activity of cryptocurrency mining, a process for acquiring new cryptocurrencies by verifying transactions on the blockchain network, is also still not specifically regulated (Disemadi & Delvin, 2021). Meanwhile, both the United States and Japan have established legal frameworks and regulations that govern various aspects of these three entities.

In Indonesia, the oversight of cryptocurrency trading now falls under the authority of the Financial Services Authority (OJK), in accordance with Law Number 4 of 2023. The OJK is empowered to supervise and regulate digital financial assets as part of innovations in the fintech sector. As a supervisory body, the OJK plays a role in ensuring that cryptocurrency trading in Indonesia complies with existing regulations. This regulation reflects the government's awareness that cryptocurrency assets, despite being new and rapidly growing, require a stringent oversight framework to prevent abuse, such as money laundering or fraud (Barone & Masciandaro, 2019). This supervisory system is like Japan's, where cryptocurrency trading is overseen by the Financial Services Agency of Japan (FSAJ). Both countries adopt an administrative oversight approach to ensure compliance among platforms and market participants with regulations, including imposing administrative sanctions for violations, ranging from warnings to license revocation.

In contrast to Indonesia and Japan, the United States has a more complex oversight structure involving multiple agencies based on the classification of cryptocurrency assets. Cryptocurrency that represents physical assets is considered securities and is regulated under the Securities Exchange Act by the Securities and Exchange Commission (SEC). To determine whether an asset qualifies as a security, the SEC utilizes a standard known as the "Howey Test." Furthermore, cryptocurrency is also treated as a commodity or virtual currency, supervised by the Commodity Futures Trading Commission (CFTC) and the Financial Crimes Enforcement Network (FinCEN). The U.S. also has a broader sanction mechanism, where agencies like the CFTC can impose administrative penalties and sue violators in court (Nabilou, 2019). These sanctions may include license cancellation, asset freezing, or even court-issued restraining orders. Meanwhile, administrative sanctions in Indonesia and Japan typically range from warnings to revocation of business licenses in case of regulatory violations.

Although the United States has a more complex and strict oversight framework through agencies such as the SEC, CFTC, and FinCEN, the challenges in overseeing cryptocurrency assets remain significant. One of the biggest challenges stems from the unique characteristics of cryptocurrency technology itself, which emphasizes anonymity and pseudonymity. Existing regulations, although well-structured in some jurisdictions like the United States, often encounter technical and operational obstacles in real-world implementation. Law enforcement agencies in various countries, including Indonesia and Japan, face similar difficulties, especially when it comes to identifying transactions conducted by users who do not clearly disclose their identities. Thus, despite the implementation of more complex and varied regulations, their effectiveness is often limited by technological barriers, particularly in the prevention of crimes such as money laundering (Jayasekara, 2021).

Law enforcement faces several challenges in monitoring and enforcing laws related to cryptocurrency transactions suspected of involvement in money laundering. Anonymity and pseudonymity are two key features that make cryptocurrencies, such as Bitcoin and Ethereum, highly attractive transaction mediums for users worldwide. Anonymity means users can transact without revealing their true identities, while pseudonymity allows users to transact using fictitious identities or aliases. While both features provide users with freedom and privacy, they also create serious challenges for law enforcement in tracking illegal activities, such as money laundering.

In cryptocurrency transactions, the identities of senders and receivers are often displayed only as a series of codes or alphanumeric addresses that do not directly correlate with the real identities of their owners. Consequently, even though the blockchain provides a transparent and permanent transaction record, the ability to trace these transactions is limited to the data available on the blockchain, which is not always tied to specific individuals or entities. Criminals can exploit this anonymity to conceal the source of funds obtained from illegal activities, such as corruption, drug trafficking, or cybercrime, and move them across borders undetected.

These advantages often make it challenging for law enforcement to conduct investigations. Unlike traditional banking systems that require financial institutions to retain customer data and report suspicious transactions, decentralized cryptocurrency trading platforms do not have similar obligations. As a result, illegal transactions involving cryptocurrencies can occur without any visible signs to oversight authorities (Masciandaro, 1999). Additionally, with the presence of additional technologies such as mixers or tumblers, which are used to obfuscate the origins of cryptocurrencies through a series of complex transactions, tracking funds becomes even more difficult.

To address these challenges, various countries are developing new regulatory frameworks that require cryptocurrency trading platforms to implement Anti-Money Laundering (AML) rules and identify their customers (KYC/Know Your Customer). However, the application of these regulations is not always straightforward, as many cryptocurrency platforms operate in a decentralized manner or outside specific jurisdictions, complicating global oversight and law enforcement. The lack of clear and comprehensive regulations regarding cryptocurrencies is a major challenge in enforcement efforts, particularly concerning the prevention of money laundering. In many countries, including Indonesia, the legal framework surrounding cryptocurrencies is still in the development stage. This creates loopholes that criminals exploit to carry out money laundering or other illegal activities without being effectively detected by law enforcement. When regulations do not provide clear rules on how cryptocurrencies should be traded, stored, and monitored, the opportunities for these assets to be used for criminal purposes significantly increase.

In Indonesia, regulations governing the trading of cryptocurrencies, such as the Regulation of the Commodity Futures Trading Regulatory Agency (Bappebti) No. 7 of 2020, only cover aspects of trading and investment, but they are still minimal in terms of oversight and action against money laundering through cryptocurrencies. Current regulations focus more on consumer protection and fraud prevention but have yet to adequately address the need to combat money laundering crimes that exploit cryptocurrencies. Consequently, law enforcement agencies struggle to monitor transaction flows and trace the flow of funds related to crimes. The gaps in this regulation also affect coordination between traditional financial institutions and cryptocurrency platforms. While traditional financial institutions are strictly regulated by AML and KYC rules, many cryptocurrency platforms, especially decentralized ones, are not subject to similar regulations. This creates oversight gaps where transactions involving cryptocurrencies can escape detection. Furthermore, given the cross-border nature of blockchain technology, criminals often take advantage of jurisdictions with less stringent regulations concerning cryptocurrencies, complicating the law enforcement process.

There is an urgent need for more comprehensive and thorough legal reforms to address these weaknesses. Developed countries like the European Union and the United States have begun to formulate tighter regulatory frameworks, including KYC requirements and suspicious transaction reporting for cryptocurrency platforms. Indonesia also needs to strengthen cryptocurrency regulations, not only concerning trading but also on oversight, law enforcement, and the prevention of money laundering offenses. This includes tightening rules regarding user identification, transaction reporting obligations, and penalties for platforms that do not comply with AML standards. The speed and flexibility of cryptocurrency transactions present major challenges for law enforcement and financial supervisors in combating money laundering activities. Cryptocurrency transactions can occur in seconds, involving participants from various parts of the world, independent of the operational hours of traditional financial institutions. These transactions take place on a blockchain, which operates 24/7 without requiring intermediaries like banks or central financial authorities. This high transaction speed makes it difficult for law enforcement to monitor and detect suspicious activities in real time. Cross-border transactions in the cryptocurrency ecosystem add complexity to oversight efforts.

A user can transfer cryptocurrencies from one country to another without geographic restrictions, and funds can change hands multiple times within minutes. This complicates authorities in one country trying to trace funds moving through several jurisdictions, especially if those countries have weak regulations or lack strong international cooperation concerning law enforcement related to cryptocurrencies. Criminals often exploit this flexibility to obscure their financial trail, moving illicit funds across various countries to evade detection. The rapid pace of transactions also complicates traditional financial institutions' compliance with AML regulations. Financial institutions typically have strict procedures for detecting and reporting suspicious transactions, yet these processes cannot keep pace with the extremely fast rhythm of cryptocurrency transactions. On the other hand, cryptocurrency trading platforms often lack similarly stringent reporting obligations, allowing suspicious transactions to occur without detection until long after they have been finalized. Because these transactions often happen outside the direct supervision of traditional financial institutions and oversight authorities, combating money laundering activities through cryptocurrencies requires a new approach. Possible solutions include enhancing international cooperation, improving monitoring technology, and implementing stricter regulations for cryptocurrency platforms, including real-time reporting obligations for large or suspicious transactions. Additionally, integrating artificial intelligence technology and data analysis can help in effectively and quickly monitoring suspicious transaction patterns.

The lack of international collaboration in combating money laundering through cryptocurrencies poses a serious challenge for law enforcement. Money laundering via cryptocurrencies often involves actors located in multiple jurisdictions, taking advantage of varying regulatory weaknesses in each country. Criminals can effortlessly transfer cryptocurrencies across borders to avoid detection and protect their illicitly sourced funds. Unfortunately, cross-border law enforcement is often hampered by a lack of cooperation between countries concerning information exchange and the enforcement of relevant regulations. One of the primary issues is the differing regulations and standards implemented in various countries. Some countries have established strict regulations regarding cryptocurrencies, while others are still in the early stages of devising comprehensive legal frameworks. This lack of harmonization complicates effective investigation efforts when cryptocurrencies move across borders. For instance, if one country lacks cryptocurrency transaction reporting obligations or adequate controls, another country attempting to trace illicit funds will face difficulties in obtaining the necessary information. This presents opportunities for money launderers to exploit gaps in the global system. Information-sharing mechanisms among law enforcement agencies in various countries are often slow and bureaucratic.

This slows down efforts to detect and prosecute money launderers using cryptocurrencies, given the rapid pace of cryptocurrency transactions. Without efficient data exchange between authorities in different countries, criminals can easily take advantage of the delays in international law enforcement systems. The lack of cooperation is also related to technical challenges. Cryptocurrencies traded through overseas exchanges are often beyond the reach of local jurisdictions. Countries seeking to trace these cryptocurrency transactions must rely on international agreements to gain access to information from other countries. However, if countries do not have strong cooperation frameworks or have not ratified international agreements concerning cryptocurrency oversight, the investigation process will be hindered.

The blockchain technology underlying cryptocurrencies offers high levels of security and privacy, yet it also presents significant challenges for law enforcement in tracking criminal activities, including money laundering. Blockchain operates through a decentralized network that records every transaction permanently in a digital ledger, but users' identities often remain anonymous or pseudonymous. While blockchain provides transparency as transactions can be viewed by anyone with access, this anonymity makes it difficult for law enforcement to identify parties involved in crimes. The security of blockchain is enhanced by complex encryption, which ensures that transactions and recorded data cannot be altered or falsified. Each block in the transaction chain is protected by strong cryptographic algorithms, maintaining data integrity. However, this encryption strength also serves as a barrier for law enforcement in penetrating money laundering networks. Decoding encryption in blockchain requires highly advanced technological resources and considerable time, slowing down the investigation and enforcement process.

Decentralization is another key feature of blockchain that creates major challenges for legal oversight. Unlike centralized traditional banking systems regulated by financial institutions or governments, blockchain is operated by a network of users distributed globally. Transactions can be conducted directly between individuals without intermediaries such as banks, thus eliminating the regulatory pathways typically used to monitor financial transactions. As a result, there is no single authority that can be held accountable or that has complete control over all transactions, making oversight considerably more difficult. Additionally, because blockchain operates across borders, this technology allows criminals to swiftly move cryptocurrencies to various jurisdictions. This complicates law enforcement's ability in one country to track the flow of funds that may traverse several nations in seconds. Without solid international cooperation and uniform regulations, efforts to combat money laundering through blockchain become increasingly complicated.

Although blockchain records every transaction, tracking these transactions often requires deep technical expertise, such as in transaction pattern analysis to identify criminal trails. These efforts necessitate specific knowledge about blockchain technology and digital forensics tools to trace well-concealed flows of funds. Without adequate technological support, law enforcement faces significant challenges in combating criminal activities in the crypto realm.

Decentralized platforms, such as Decentralized Exchanges (DEX), allow cryptocurrency transactions to be executed without intermediaries like banks or traditional financial institutions. On these platforms, users can transact directly, eliminating the third-party roles that typically function as monitoring mechanisms. In traditional financial systems, financial institutions have an obligation to report suspicious activity and conduct regular audits. However, with decentralized platforms, there is no single authority to monitor the transactions. Without a clear regulatory authority, decentralized platforms offer greater freedom to users, including criminals seeking to hide their tracks. They can exploit the anonymity of these platforms to conduct money laundering and other illegal transactions without being subjected to the reporting mechanisms present in traditional financial systems. This becomes a significant challenge for law enforcement agencies, as there is no entity accountable for providing information about transactions taking place on such platforms. The global and cross-border nature of decentralized platforms exacerbates the situation, as transactions can be executed by parties located in various jurisdictions with significantly different laws. Without internationally applicable regulatory standards, decentralized platforms enable criminals to execute transactions beyond the oversight of local authorities, making it difficult for law enforcement to trace the flow of funds involving multiple countries.

Another challenge in law enforcement related to cryptocurrency assets is the limited technological expertise among law enforcement personnel. Blockchain and cryptocurrency technologies are complex and require a deep understanding of cryptography, distributed networks, and digital transaction mechanisms. Law enforcement agencies often lack the specialized training or expertise necessary to address crimes involving such technology. This results in slow and ineffective investigation processes, particularly in cases of money laundering perpetrated through cryptocurrency transactions. The shortage of human resources trained in blockchain technology hampers the ability of agencies to keep up with increasingly sophisticated criminal modus operandi. Additionally, budget limitations and technological infrastructure also hinder law enforcement institutions' capability to invest adequate time and resources in developing technical expertise. This situation leads to a reliance on external experts or specialized agencies, which often reduces investigation efficiency. Without adequate training, law enforcement agencies struggle not only to detect crimes in the digital realm but also to gather valid digital evidence for court proceedings. This worsens the situation in prosecuting criminals using cryptocurrencies as a means for money laundering, as many cases end without punishment due to a lack of strong technical evidence. Thus, enhancing technological expertise among law enforcement personnel is an urgent need to ensure they can effectively tackle the challenges presented by advanced technologies like blockchain and cryptocurrencies.

Efforts to address regulatory challenges related to sanctions and oversight of cryptocurrency transactions suspected of involvement in money laundering require a more coordinated approach among regulators, law enforcement agencies, and industry participants. One of the primary efforts is to strengthen Anti-Money Laundering (AML) and Know Your Customer (KYC) regulatory frameworks. Implementing stricter KYC rules across cryptocurrency platforms can help identify parties involved in suspicious transactions. Furthermore, technology-based oversight, such as using monitoring algorithms and blockchain analysis, can assist regulators in tracking suspicious transaction activities and identifying patterns that may potentially relate to money laundering (Marzuki, n.d.).

In terms of sanctions, countries need to strengthen efficient and rapid law enforcement mechanisms. Oversight agencies, such as the Commodity Futures Trading Commission (CFTC) in the United States, have implemented administrative sanctions that include asset freezing and revocation of operating licenses for platforms or individuals involved in money laundering activities. Efforts need to be adopted and enhanced in Indonesia and other countries by empowering regulators to swiftly impose sanctions. Additionally, international cooperation through cross-border collaboration, such as through the Financial Action Task Force (FATF), becomes crucial in addressing money laundering activities that often involve global transactions. Improving the capacity of law enforcement agencies to analyze and monitor cryptocurrency transactions is also an important step toward more effective oversight. Agencies need training to utilize advanced technology capable of tracking blockchain transactions and recognizing illegal activities, even when perpetrators use anonymity or pseudonymity features. Moreover, developing a more specific legal framework to regulate new innovations such as Non-Fungible Tokens (NFTs) and Stablecoins will help fill regulatory gaps, ensuring that all forms of digital assets are comprehensively regulated and safeguarded against abuse. This effort must also be accompanied by cooperation between the public and private sectors, including cryptocurrency platforms, to share information regarding suspicious transactions. Cryptocurrency service providers should be proactive in reporting suspicious activities to authorities and implementing adequate AML procedures. This overall strategy is expected to effectively tackle oversight and law enforcement challenges regarding money laundering through cryptocurrencies by leveraging more adaptive regulations, advanced monitoring technologies, and cross-sector and international collaboration.

CONCLUSION

Cryptocurrency serves two primary functions: as a medium of exchange and as a commodity. In Indonesia, cryptocurrency is not recognized as a legal means of payment under Law Number 7 of 2011, which designates the rupiah as the sole legal tender, and current regulations, including those from BAPPEBTI, only classify cryptocurrency as a commodity. Despite this limitation, the use of cryptocurrency for payments and investments has grown significantly due to its decentralized, anonymous nature and transaction flexibility. However, these characteristics also present substantial challenges for law enforcement, particularly in combating money laundering and terrorist financing, as the anonymity of cryptocurrency complicates the tracking of illegal activities. Blockchain technology's complexity, coupled with limited international regulatory frameworks, exacerbates these issues, often involving cross-jurisdictional challenges. The emergence of digital assets such as the planned Digital Rupiah further highlights the need for rigorous oversight to prevent potential misuse. Addressing these challenges requires comprehensive policy reforms, including strengthening Anti-Money Laundering (AML) and Know Your Customer (KYC) frameworks, implementing advanced monitoring technologies, and fostering international cooperation. Additionally, regulatory measures must expand to encompass innovations like Non-Fungible Tokens (NFTs) and Stablecoins, ensuring the entire digital asset ecosystem is well-regulated and safeguarded against abuse.

REFERENCES

Almeida, H., Pinto, P., & Vilas, A. F. (2023). A Review on Cryptocurrency Transaction Methods for Money Laundering. *ArXiv Preprint ArXiv:2311.17203*.

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics*, *47*, 233–254.

Disemadi, H. S., & Delvin, D. (2021). Kajian Praktik Money Laundering dan Tax Avoidance dalam Transaksi Cryptocurrency di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(3), 326–340.

Firdaus, S. P. (2023). The Urgency of Money Laundering Policy Reform for Digital Rupiah Implementation. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering The Financing of Terrorism*, *2*(1), 58–82.

Group, E. (2022). E. Group, "FinTech Cooperation and Associated Cybercrime Typologies and Risk," Prepared by the Information Exchange Working Group, p. 16, 2022. *"FinTech Cooperation and Associated Cybercrime Typologies and Risk,."*

Handa, R. K., & Ansari, R. (2022). Cyber-laundering: An emerging challenge for law enforcement. *Journal of Victimology and Victim Justice*, *5*(1), 80–99.

Indonesia, B. (2008). B. Indonesia, Laporan Sistem Pembayaran dan Pengedaran Uang, Jakarta: Bank Indonesia, 2008. *Laporan Sistem Pembayaran Dan Pengedaran Uang*.

Jayasekara, S. D. (2021). Deficient regimes of anti-money laundering and countering the financing of terrorism: agenda of digital banking and financial inclusion. *Journal of*

Money Laundering Control, *24*(1), 150–162.

Kurniawan, I. (2012). Perkembangan Tindak Pidana Pencucian Uang (Money Laundering) dan Dampaknya Terhadap Sektor Ekonomi dan Bisnis. *Jurnal Ilmu Hukum Riau*, *3*(2), 9139.

Lin, D., Wu, J., Yu, Y., Fu, Q., Zheng, Z., & Yang, C. (2024). DenseFlow: Spotting Cryptocurrency Money Laundering in Ethereum Transaction Graphs. *Proceedings of the ACM on Web Conference 2024*, 4429–4438.

Marzuki, P. M. (n.d.). A. Pendekatan Masalah. *PERAN LEMBAGA PERLINDUNGAN SAKSI DAN KORBAN (LPSK) DALAM PERLINDUNGAN HUKUM TERHADAP*, *43*.

Masciandaro, D. (1999). Money laundering: the economics of regulation. *European Journal of Law and Economics*, *7*, 225–240.

Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291.

Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *9*(11).

Puspasari, S. (2019). *Perlindungan Hukum bagi Investor pada Transaksi Aset Kripto dalam Bursa Berjangka Komoditi*. Universitas Airlangga.

Rani, D. A. M., Sugiartha, I. N. G., & Karma, N. M. S. (2021). Uang Virtual (Cryptocurrency) Sebagai Sarana Tindak Pidana Pencucian Uang dalam Perdagangan Saham. *Jurnal Konstruksi Hukum*, *2*(1), 19–23.

Rohman, M. N. (2021). Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia. *Jurnal Supremasi*, 1–10.

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. *ArXiv Preprint ArXiv:1908.02591*.

Wu, J., Lin, D., Fu, Q., Yang, S., Chen, T., Zheng, Z., & Song, B. (2023). Towards Understanding Asset Flows in Crypto Money Laundering Through the Lenses of Ethereum Heists. *IEEE Transactions on Information Forensics and Security*.