Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany)

Tiara Putri[1], Amiludin[2], Dwi Nurfauziah Ahmad[3], Hidayatulloh[4]
[1,2,3] Faculty of Law, Universitas Muhammadiyah Tangerang, Indonesia
[4] Faculty of Law, University of Miskolc, Hungary
Corresponding author's email : tsamanytrans@gmail.com

Article Information

Submitted : February 27, 2023
Reviewed : May 5, 2023
Revised : July 10, 2023
Accepted : August 2, 2023

Keywords: cryptocurrency; comparative law; money laundering

DoI:10.20961/yustisia.v12i2.71835

Abstract

Cryptocurrency as a virtual currency managed by a decentralized system makes it immune to government interference and allows it to transact under pseudonyms. This has the potential for cybercrime and illicit transactions, especially money laundering. This study aims to compare legal instruments in Indonesia, the US, and Germany regarding the use of cryptocurrency as a money laundering tool and to analyze the readiness of Indonesia to respond to this crime. This paper is normative legal research conducted using a comparative and statutory approach. These findings show that the US and Germany have extensively regulated crypto. In the US, Crypto transactions are considered MSB, subject to BSA compliance. Each transaction must comply with AML, KYC, and CIP requirements. In Germany, Cryptocurrency is considered a personal asset. The crypto trading must meet the KYC and AML requirements. Indonesia needs advanced regulations because crypto is only considered an investment asset. The investigation is difficult because cryptocurrency is transacted pseudonyms, so connecting pseudonyms with real people is challenging.

I. Introduction

Technological advances have an impact not only on the economic sector but also on the development of criminal acts, including money laundering. Money laundering is no longer only done traditionally. Currently, methods of committing money laundering have developed through cryptocurrencies (Rani et al., 2021). Cryptocurrency is utilized for more than just investment purposes. However, its use is also an asset that facilitates money laundering. Cryptocurrencies make it easier for perpetrators to hide that they got money illegally by making it look like a legal asset. Cryptocurrency can easily facilitate

cross-border transactions, even anonymously, which has the potential for money laundering (Mabunda, 2018). This will cause financial institutions and governments to worry because any central authority does not monitor it.

In 2016, Heather Morgan and Ilya Lichtenstein laundered cryptocurrency money in the United States. In that crime, the two laundered the proceeds of 119,754 Bitcoins stolen from the Bitfinex Platform, leading to their indictment of conspiracy to commit money laundering, which carries a maximum prison sentence of 20 years (Ministry of Justice, 2022a). Then, in Poland, there was a case of money laundering using cryptocurrency involving Crypto Capital Corporation (CCC). Polish police arrested CCC President Ivan Manuel Molina Lee after being found guilty of laundering money for Colombian drug cartels by exchanging cash for crypto through Bitfinex (Biggs, 2019). Furthermore, in 2021, in Sydney, there was a case of money laundering via cryptocurrency worth more than **$5 million**. In this case, detectives from the Cybercrime Squad are prosecuting at least six perpetrators. The perpetrators allegedly laundered Australian currency, which police said was "illegal" because it came from selling illegal drugs and then converting it into Bitcoin (Ward,2007). In Indonesia, a similar case occurred at Asabri Ltd. When investigating the Asabri Ltd money laundering case which involved Jimmy Sutopo, Benny Tjokrosaputro, and Heru Hidayat, the Attorney General's Office found the three suspects often made stock transactions using Bitcoin (Rahma, 2021).

As a type of cryptocurrency, bitcoin is a new payment system that uses an entirely digital currency and a decentralized peer-to-peer payment network (F. N. A. Wijaya, 2019). There are other popular cryptocurrencies besides Bitcoin (BTC), but they exist only as digital assets. The Indonesian government emphasizes that the Rupiah is the only legal tender in Indonesia. As stated in Law Number 7 of 2011 regarding Currency, the Rupiah is the only legal tender issued in notes and coins with distinct characteristics in Indonesia. Therefore, using crypto assets as a medium of exchange for legal transactions in Indonesia would be illegal. Moreover, Bank Indonesia (BI) Regulation Number 20/6/ PBI/2018 states that electronic money must have the following elements:

a. Issues are published based on the value of money paid in advance to the publisher;

   This element obliges the issuer to disseminate the value of electronic money based on user advances to the issuer. Electronic money users must first exchange cash or electronic funds with the issuer so that the value can be stored in electronic money.

b. Money values are stored electronically on a media server or chip;

   This element stipulates that e-currency values must be stored in electronic format, either on a media server or on a chip embedded in a card or other device. Cryptocurrencies are not stored on media servers or chips but on a blockchain system.

c. The value of electronic money managed by the issuer is not a deposit as referred to in the Act that regulates banking.

Because electronic money is stored electronically on the card after it has been deposited at the issuing bank, it is not a deposit product. Instead, cryptocurrency was stored on the blockchain. Unsaved cryptocurrency is recorded electronically on a card issued by a bank.

Thus, cryptocurrency is not electronic money that can be used as a legal tender in Indonesia. The non-recognition of cryptocurrency in Indonesia as a legal medium of exchange protects the public against potential systemic losses (Sajidin, 2021).

The Crypto Spot Asset Framework defines Cryptocurrency as a digital representation of value that functions as a medium of exchange or a unit of account and is not issued by a government agency (Blandin et al., 2019). There is a connection between cryptocurrency and money laundering. Cryptocurrency has attracted the attention of the world community with its ability to support money laundering and other criminal acts. Cryptocurrency allows anonymous transactions to occur, in this case it is used to cover up the true identity of its users. Then, cryptocurrency is not required to go through a licensed bank or even a third party. On the other hand, money can be transferred freely and independently without regard to the purpose or legality of the transaction (Forgang, 2019). This nature of cryptocurrency supports cryptocurrency exchanges to facilitate money laundering activities.

Cryptocurrencies have limited functionality as digital assets and serve as a remittance and investment commodity only. In addition, its use is limited to electronic media. Cryptocurrency also enables perpetrators to hide the results of their crimes because they are not subject to Anti-Money Laundering (AML) principles and Know Your Customer (KYC). Despite that, cryptocurrency is synonymous with using pseudonyms, obscuring the culprit's identity. However, some opportunities allow actors to make transactions anonymously, meaning they cannot be identified using coin mixers and decentralized exchanges (DEXs) (Stobierski, n.d.).

Data on cryptocurrency money laundering activities, based on the Chainalysis Team from 2017 to 2021, as follows (Chainalysis Team, 2022):

a. Cybercriminals, through centralized exchanges, had laundered more than $33 billion in cryptocurrency since 2017.
b. The centralized exchange since 2018 for the first time, did not receive most of the funds sent via banned addresses last year and only accepted 47%.
c. According to the latest data from CoinShares, the total inflow of investors to cryptocurrency funds and products is up more than 600% from 2019 and has reached $5.6 billion so far this year.
d. In 2020, law enforcement may have reduced the concentration of money laundering activities as only 270 deposit service addresses accept 55% of all cryptocurrency sent from prohibited addresses.

e. As of 2021, the amount of cryptocurrency laundered by cybercriminals from restricted addresses to addresses hosted by such services, reached $8.6 billion. Compared to the 2020s, around 54% with fewer services used in 2021, the concentration of money laundering sent from restricted addresses increases to 58%.

The Government of Indonesia has realized the need for regulation regarding cryptocurrency. Through the Commodity Futures Trading Supervisory Agency (BAPPEBTI), the government has regulated crypto assets in Commodity Futures Trading Supervisory Agency Regulation Number 5 of 2019 concerning Technical Provisions for Organizing the Physical Crypto Asset Market on the Stock Exchange Futures. Nevertheless, this regulation is considered ineffective due to the money laundering perpetrator's widespread use of cryptocurrency assets, causing the country to lose its wealth without a trace. The integrity of the financial system and economic stability are threatened because these crimes harm the social sector, nation, and government (Wardhana & Sularto, 2022).

In carrying out money laundering through cryptocurrency, enforcement tends to be difficult because the movement of money in cryptocurrency is easy to move and difficult to track (Utami & Astuti, 2022). Current regulations are not effective enough to deal with the complexities of cryptocurrencies and the potential risks as a means of money laundering, so comprehensive legislation is needed to deal with this crime. Preventive efforts are needed considering how significant the impact of money laundering through cryptocurrency is on state finances. So, the government needs to focus more on the steps that can be taken to get rid of crimes that use this cryptocurrency. The United States and Germany already have strict regulations regarding efforts to handle cryptocurrency as a tool used in money laundering.

Currently, the implications of crypto coins for global AML efforts stem less from the threat of their illegal use as a digital currency. Blockchain technology is one of the fundamental opportunities that exist today. The Financial Action Task Force (FATF) has formulated a risk-based approach involving the coordination of anti-money laundering efforts. Such a risk-based approach effectively balances the threats and opportunities that crypto coins present. There is a critical need for ongoing monitoring and investigation into the wider ethical implications raised by crypto coins to combat money laundering (Campbell-Verduyn, 2018).

This study examines the use of cryptocurrencies as a money laundering tool, its regulation, and law enforcement in Indonesia compared to laws related to cryptocurrencies in effect in the United States and Germany. Based on credible facts, this research provides stronger and optimal efforts to prevent and eradicate money laundering through cryptocurrency in Indonesia by examining the potential for absorption of efforts that the United States and Germany have made. Optimal efforts to eradicate this crime can be started by comprehensively regulating cryptocurrency as a money laundering tool and other criminal acts facilitators in Indonesia's law and by forming specific agencies

with qualified backgrounds and abilities, as applied in the United States and Germany. As of 2021, global adoption of cryptocurrencies has grown by over 2300% since 2019 and over 881% in 2020, leading North America, Western Europe, and East Asia to load their asset classes (Chainalysis Team, 2021). According to the 2021 crypto-ready index, which determines countries' readiness to adopt crypto, the United States ranks first with a total score of 7.13/10, while Germany ranks 9th with a total score of 5.93/10. The index was analyzed based on several factors as follows: the amount of crypto in the country, its accessibility to the general public, legal attitudes regarding ownership of ownership, and whether or not it can be used in banks and the state's interest in cryptocurrencies (Crypto Head, 2021). Then, based on a study by Coincub, namely the Coincub Global Crypto Ranking, Germany was declared the most crypto-friendly country in the world for Q1 2022 with a first rank. Based on the same study, the United States was ranked third in the Coincub Global Crypto Ranking (Coincub, 2022). Based on these data, the United States and Germany had proven their seriousness in adopting cryptocurrency, and both of them have a ready and supportive environment to deal with cryptocurrencies, especially in dealing with money laundering using crypto assets.

Related to the focus of the study are journal articles, publications, or previous research that show more analysis from the perspective of trading and bitcoin only, such as a study conducted by Anak Agung Ngurah Wisnu and Ni Ketut Supasti Dharmawan with the title "Legality of Crypto Asset Investment in Indonesia as a Digital Commodity and Payment Instrument" (Wisnu & Dharmawan, 2021), and Muhammad Najibur Rohman, entitled "Normative Judicial Review of Cryptocurrency Regulations" (Rohman, 2021). None of these studies discuss money laundering transactions carried out through cryptocurrencies, which focus on comparisons of regulation and law enforcement between Indonesia, the United States, and Germany and on progressive steps that can deal with and prevent the spread of this crime. This research is very important because it deals with cryptocurrencies, which are very complex and allow anonymous transactions to occur, so this crime continues to spread and is difficult to control. The absence of cohesive regulations on cryptocurrencies is enticing criminals to find alternative ways to launder the proceeds of their crimes in cryptocurrencies (Anika, 2019).

This legal research employs normative legal research methods that focus on library materials to answer the problem formulation (Soekanto, 2020). The approaches used are a statutory approach and a comparative approach. The statutory approach examines regulations regarding cryptocurrency as a money laundering tool in the United States, Germany, and Indonesia. In addition, a comparative approach is carried out by comparing the laws in one country with those in other countries (Marzuki, 2013). The comparative approach in this study will examine regulations and law enforcement related to cryptocurrency assets as a money laundering tool in Indonesia, which are not yet sufficiently qualified compared to regulations in the United States and Germany, which are more progressive in dealing with this matter. The development of the crypto market goes hand in hand with the growth of academic research. Until now, there is no

known field of study that has received significant attention, is relatively uncharted, and has changed substantially. This research is descriptive-analytical in nature, namely by using writing to describe the problem based on existing data and then analyzing it to draw conclusions. It analyzes the semantic topics of top journal publications to answer these questions.

II. Indonesia Legal Framework of the Cryptocurrency and Money Laundering

Money laundering has existed in the United States since 1830. The term "money laundering" was used when one of the biggest mafias in the United States in the 1930s, Al Capone, hid his proceeds from prostitution, extortion, and selling illegal liquor. In order to deceive the government, the mafias set up a laundry company in which the parties mix the money obtained from the proceeds of crime so that it looks as if the money was obtained legally (Husein & K, 2020). The method chosen to turn the "dirty" money into "clean" money tends to vary and continues to grow, including doing business activities, buying buildings or other assets, and transferring money to other accounts. Money laundering-related crimes can range from narcotics offenses to corruption offenses to terrorism funding offenses, among other things.

The rise of money laundering cases has become a global spotlight, giving rise to various efforts to prevent and deal with this crime. 1988 was the beginning of the policy or principle that until now has been closely related to the activities of financial institutions, especially banks, namely "Know Your Customer" (KYC). This policy is established by representatives of central banks and regulatory agencies worldwide through the Basel Committee on Banking Regulations and Supervisory Practices (Rajagukguk, 2005). Furthermore, these states agreed to form an international organization that focuses on preventing and eradicating money laundering, known as the Financial Action Task Force on Money Laundering (FATF), at the G-7 meeting in Paris (FATF, 2002). FATF's primary mission is to develop international recommendations for eradicating money laundering. Indonesia is still an observer and not yet a member of the FATF. In 1997, this state became a member of the Asia-Pacific Group (APG) on Money Laundering, established in Bangkok through the Fourth Asia-Pacific Money Laundering Symposium. Like the FATF, APG is an autonomous anti-money laundering institution with a regional scope (FATF, n.d.). Its existence in the Asia/Pacific region facilitates the implementation of the FATF's forty recommendations and eight special recommendations within a smaller scope. It facilitates cooperation among governments in countries combating money laundering.

Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes, sets the rules for money laundering in Indonesia. The Criminal Procedure Code (CPC) and the Money Laundering Law look at investigations from different points of view. The CPC investigation still focuses on a "person" suspected of having done something wrong. The Money Laundering Law has a progressive perspective, namely,

making "assets" into objects. The concept of the Money Laundering Law is known as "follow the money" (Ginting, 2021). The excellent impact is that investigators can confiscate money suspected of being the proceeds of a crime for investigation without having to look for suspects first.

Cryptocurrencies are considered one of the most popular methods of money laundering. Cryptocurrency is designed with very complex cryptography and methods, making it difficult to counterfeit (Pramudiya, 2021). In computer science, cryptography is the study of ways to conceal information. A secret message is randomized into a message that appears to be formless and conveyed to the intended recipient using cryptography (D. A. Wijaya, 2016). In contrast to fiat money, cryptocurrency is a truly absolute virtual money wheel. The decentralized distribution of cryptocurrency with a peer-to-peer network system does not allow Bank Indonesia to access it freely (Muttaqim & Apriliani, 2019). This means no legal state financial authority supervises cryptocurrencies, in which transactions are one-way and directly between the perpetrators. It can be understood if money laundering perpetrators take steps to commit crimes through investing in exchangers because, in truth, money laundering is a white-collar crime, so the perpetrators of crimes are people who have high intellect and expertise (Adiyatma & Maharani, 2020).

The existence of cryptocurrency as a virtual currency was regulated by Bank Indonesia (BI) regulations. In accordance with Article 34 (a) PBI Number 18/40/ PBI/2016, regarding the implementation of payment transaction processing, payment system service providers in Indonesia will not process payment transactions involving virtual currency. Based on BI regulations, Number 19/12/PBI/2017 concerning the application of financial technology prohibits the use of virtual currency payment systems by financial technology operators because cryptocurrencies are not legal tender in Indonesia. In addition, Article 62 of PBI Number 20/6/PBI/2018 concerning electronic money prohibits electronic money operators from utilizing, connecting, receiving, and processing virtual currency transactions. Then, PBI Number 23/6/PBI/2021 concerning payment service providers prohibits payment service providers from receiving, processing, or connecting payment sources originating from virtual currency.

Based on Article 1 of the Regulation of the Minister of Trade of the Republic of Indonesia Number 99 of 2018 concerning the General Policy for the Implementation of Futures Crypto Asset Trading and Commodity Futures Trading Regulatory Agency (BAPPEBTI) Regulation Number 3 of 2019 concerning commodities that can be used as the subject of Futures Contracts, Sharia Derivative Contracts, and/or Other Derivative Contracts Traded on Futures Exchanges, Crypto Assets in Indonesia are defined as commodities that can be used as the subject of futures contracts traded on Futures Exchanges. A total of 299 types of crypto assets that can be physically sold on the crypto asset market are mentioned in Appendix II of BAPPEBTI Regulation Number 7 of 2020 concerning the establishment of a list of crypto assets that can be traded on the physical crypto asset market. The physical market for crypto assets in question is the physical

market for crypto assets which is held using electronic facilities owned by physical traders of crypto assets for selling or buying crypto assets and market supervision is carried out by futures exchanges as referred to in Article 1 of BAPPEBTI Regulation Number 13 of 2022 concerning Amendments Based on CoFTRA Regulation Number 8 of 2021 concerning Guidelines for Organizing Crypto Asset Physical Market Trading on Futures Exchanges. BAPPEBTI Regulation Number 13 of 2022 also discusses crypto assets as intangible commodities in digital form, using cryptography, information technology networks, and distributed ledgers to regulate the production of new units, verify transactions, and protect transactions without the interference of other parties.

Central bank authorities strictly prohibit the use of cryptocurrencies. Through BAPPEBTI, the Ministry of Trade decided that cryptocurrency is a digital asset in commodity trading. BI will issue Central Bank Digital Currency (CBDC), a blockchain-based virtual currency whose circulation will be monitored directly by BI (Departemen Komunikasi Bank Indonesia, 2022).

Even though cryptocurrencies provide pseudo-anonymity, if the perpetrator transacts through a decentralized exchange (DEX), it will allow anonymous transactions. This anonymity is the main attraction for money laundering perpetrators. There are no identity details for the owner of cryptocurrency assets. Identity is only given in the form of a set of codes. Seeing the confidentiality of identity in cryptocurrencies, which is quite capable, the principle of "follow the money" and "follow the suspect" seems outdated and irrelevant in the investigation process because the form of "money" used is very different and challenging to trace. Furthermore, a method seeks to complicate identifying money laundering through cryptocurrency, known as "Bitcoin Laundry."

Bitcoin laundry can obscure transaction details, making identification and follow-up difficult. The method used is through a coin mixer, where a person's digital coins will be mixed with other people's digital coins in a tumbler so that the coins will be challenging to separate and identify which coins come from one user's wallet and another. This mode aims to obscure the traces of transactions (Nelson, 2022).

A coin mixer is a service whose job it is to "mix" Bitcoin and other virtual currencies at random to obscure the origin and destination of transactions so that tracking by law enforcement officials will encounter difficulties. In the coin mixer mechanism, the criminal proceeds of the perpetrator are used to buy virtual currency on the exchange. Then the perpetrator will send the virtual currency to the coin mixer service, which will make the virtual currency of the perpetrator anonymous, and every transaction will be challenging to trace. Furthermore, a new virtual currency set mixed with other virtual currencies will be randomly sent back by the coin mixer to the perpetrator so that there are no traces of previous transactions (Ridwan, 2022). "Follow the money" as a legal effort to combat money laundering becomes more difficult to implement. The coin mixer service itself will be difficult to process legally. In Indonesia, cryptocurrencies as a money-laundering tool do not yet have specific regulations, nor do coin mixers. The absence

of rules governing coin mixers makes it challenging to implement law enforcement on this matter because there needs to be a clear legal basis to serve as a reference for law enforcement to create legal certainty and avoid multiple interpretations.

In essence, it is difficult for cryptocurrency to become the official national currency in Indonesia. This is because national and economic policies do not influence the fluctuating price of digital currency, so its value cannot be maintained (Sam et al., 2022). To be used as a payment system, cryptocurrency must facilitate the transfer of funds safely, efficiently, and quickly (Kusumaningtyas & Derozari, 2019). Cryptocurrency is considered incapable of fulfilling the security system in the payment system in Indonesia. This has been proven by fraud and bitcoin theft at Mt.Gox, the world's largest bitcoin exchange, in 2014, indicating a low level of security for bitcoin storage.

Indonesia has adopted the "Travel Rule," which has been recommended by the FATF. The "Travel Rule" rules in Indonesia are regulated in the BAPPEBTI Regulation Number 8 of 2021. This regulation stipulates that a virtual asset service provider will send the sender and recipient information to the authorized party when conducting cryptocurrency transactions in Rupiah worth more than USD 1000. This regulation aims to mitigate the risk of using crypto for money laundering. Protection and tracking efforts for the flow of cryptocurrency funds in Indonesia are still limited to implementing general principles. Provisions regarding the provision of information were initially only regulated in general in Article 9 of Law Number 11 of 2008 of the Republic of Indonesia concerning Information and Electronic Transactions. Based on the policy, every business actor that offers products through an electronic system should provide complete and accurate information regarding the contract term, producers, and products offered. However, there are provisions that require buyers of cryptocurrency assets to make purchases with their identity (KTP or passport) and require cryptocurrency marketplaces, such as Indodax, to verify identity. This is confirmed by BAPPEBTI Regulation Number 8 of 2021 on Guidelines for Organizing Crypto Asset Physical Market Trading on Futures Exchanges.

These provisions do not necessarily rule out the possibility of buying cryptocurrency without an identity. The existence of a decentralized exchange (DEX) allows cryptocurrency purchases without identity verification, as required for the application of KYC principles (Lin, 2019). Some DEXs often used to maintain anonymity include Block DX, ByBit, Changelly, and IDEX. Asset owners' high interest in trading and storing cryptocurrency assets on DEX shows that anonymity is an advantage of cryptocurrency that asset owners continue to strive to maintain. Thus, this is the main obstacle to investigating money laundering through cryptocurrency nationally and globally.

Indonesia still needs advanced regulations regarding cryptocurrency law enforcement mechanisms as a tool used for money laundering. Because the investigation process itself is not easy, considering that cryptocurrency is transacted anonymously and cryptocurrency as a money laundering tool has not been regulated extensively and

comprehensively in Indonesian law. The confiscation of cryptocurrency assets is still guided by the CPC, which is irrelevant because cryptocurrency assets are "virtual" and can be stored online, making them easy to move without knowing regional boundaries. Normatively, law enforcement and the confiscation of crypto assets suspected of being used for money laundering are based on Article 3 of Law Number 8 of 2010, concerning the Prevention and Eradication of Money Laundering Crimes, which regulates the following:

> "Anyone who transfers assigns, spends, pays, donates, entrusts, and exchanges currencies, securities, **or other acts on assets which are known or suspected as the result of criminal acts** referred to in Article 2 paragraph (1) to hide or disguise the origin of the assets is punished for money laundering crimes with a maximum prison sentence and a fine of 20 (twenty) years and IDR 10,000,000,000,00 (ten billion rupiahs), respectively."

Exchanging criminal proceeds into cryptocurrency to disguise or hide the origin of assets can be classified as "or other acts on assets which are known or suspected as the result of criminal acts." Therefore, confiscating these cryptocurrency assets fulfills the category "which may be subject to confiscation" in Article 39, paragraph 1 of the CPC. Although the crime can be enforced based on Article 3 of the Money Laundering Law, legal ambiguity exists. Cryptocurrencies do not include securities or types of money as defined in Article 3 of the Money Laundering Law. The existence of crypto assets only depends on the element of the article "other actions" as a manifestation of the principle of legality if there is a new method of money laundering (Nurcholis et al., 2021). In general, handling money laundering and pursuing assets is carried out through Asset Tracing and Recovery (ATR) activities, including profiling suspect assets to confiscate. Asset profiling must be carried out carefully, measurably, and precisely because, through this profiling, it is necessary to know who owns the asset, the value of the asset, and when the asset was acquired. As a result of the anonymity inherent in cryptocurrencies, as previously described, a series of investigations, including confiscation, become complicated when applied to cryptocurrency assets. This obstacle is in the spotlight around the world. In this case, the United States and Germany already have specific mechanisms regarding cryptocurrencies as a tool for money laundering.

III. Comparison of Law Enforcement on Cryptocurrency Assets as a Money Laundering Tool in the United States and Germany

A. United States

Cryptocurrency has become a major focus in the United States due to its widespread use in money laundering crimes. At the federal level, some of the focus is on the administrative level, including the Federal Trade Commission, the Securities and Exchange Commission (SEC), the Department of the Treasury

through the Internal Revenue Service (IRS), the Commodity Futures Trading Commission (CFTC), the Office of the Comptroller of the Currency (OCC), and the Financial Crimes Enforcement Network (FinCEN) (Dewey & Patel, 2023).

The Department of the Treasury, as the executive branch of the federal government responsible for state finances, collects taxes through the IRS. (Amadeo, 2022). The IRS classifies virtual currency as property for federal income tax purposes, so any exchange gains or losses are taxable (Enyi & Le, 2017). The exchange and use of convertible virtual currency has tax consequences that result in tax liability. As digital representations of value that serve as a medium of exchange and store of value, cryptocurrencies operate similarly to "real" currencies in certain environments, namely coins and banknotes of the United States or other countries that are designated as legal tender and circulated, but does not have legal tender status in any jurisdiction (Internal Revenue Service, 2014).

The Bank Secrecy Act (BSA) requires financial institutions to assist US government institutions in preventing and detecting money laundering by identifying and assessing customer risks through KYC and Customer Identification Program (CIP) , saving recorded cash purchases that can be negotiated, and reporting all suspicious activities related to embezzlement, money laundering, and other criminal activities (Lemire, 2022).

FinCEN issued a notification in 2013 stating that all exchanges and management of virtual currency are subject to the BSA, Title III of the USA Patriot Act, and must register as a Money Service Business (MSB) (Budhi, 2021). This regulation seeks to prevent the use of virtual currency for illegal activities such as money laundering, tax evasion, and prohibited funding. The United States does not recognize cryptocurrencies as legal tender. Exchanges of cryptocurrencies are legal and occur under the BSA. Providers of cryptocurrency exchange services must register with FinCEN, implement an AML program, maintain appropriate records, and file pertinent reports with the relevant authorities.

Fluctuations are an important factor in reducing the use of cryptocurrencies for money laundering. The volatility of the decline in the price of cryptocurrencies can be attributed to human factors such as fraud and international market fluctuations, in addition to other causes that contribute to the instability of the underlying cryptocurrency system (Krishnan, 2020). However, cryptocurrencies are still widely used today. Based on data obtained by Finbold, the number of crypto users will increase to 417.5 million in 2023, an increase of 112.5 million users compared to 2022 which recorded 305 million users (Baltrusaitis, 2023). Although crypto values are prone to fluctuations, laundering money through crypto is still easier. The money laundering stage consists of placement, layering and integration stages. The perpetrator places funds in a non-monetary

instrument by buying cryptocurrency during the placement phase. In addition, at the layering stage, the perpetrator performs a series of transactions to hide the origin of the funds by transferring them to another cryptocurrency account (Kocegarovas, 2022). Then in the final stage, namely integration, all funds are hidden. It is not easy to track cryptocurrency during an investigation. In response to the global problem of tracking money laundering through cryptocurrency, the United States, as a member of the FATF, employs a report on "Virtual Assets Red Flag Indicators" to detect suspicious virtual asset transactions. These indicators include (FATF, 2020):

1. Transactions involving multiple types of virtual assets, especially private coins or DEXs, which offer more secure anonymity;
2. Running virtual assets that initially operate on a transparent and public blockchain, such as Bitcoin, and then exchange them for private coins;
3. Users use the Virtual Asset Service Providers (VASP) platform by registering their internet domain names through a proxy or DNS that can change the domain owner, etc.

These indicators can help detect the flow of funds from virtual assets used to facilitate money laundering. Even so, similar to Indonesia, which has difficulty tracking cryptocurrency transactions that have been mixed, apart from identifying those indicators of transactions, the United States has also formed a National Cryptocurrency Enforcement Team (NCET). The NCET engages prosecutors with experienced money laundering, cryptocurrency, and cybercrime backgrounds to address issues surrounding the illegal misuse of cryptocurrencies and digital assets. The NCET also investigates, identifies, and pursues cases from the money laundering department involving the illegal use of digital assets. NCET focuses on infrastructure providers, virtual coin mixing services, and virtual currency exchanges for illegal purposes. NCET is leading efforts to eradicate the use of cryptocurrencies as a tool for money laundering and other crimes against the law. This effort was carried out by NCET in coordination with private industry, regulatory agencies, and law enforcement partners both domestically and internationally. NCET focuses on addressing this issue, particularly in investigations and prosecutions (Department of Justice, 2022b).

There have been several cases of cryptocurrency being used as a tool for money laundering in the United States. The one that has gotten the most attention is the case of Liberty Reserve, a money-transfer service provider, which occurred in 2013. Liberty Reserve customers are not required to include their identity. In this case, Liberty Reserve customers exchange their money for the virtual currency that Liberty Reserve has provided. Then, that digital money is converted back to cash. The company receives $ 2.99 for each transaction.

The United States Department of Justice says that the mechanism has been used to process 78 million transactions with a combined value of up to $8 billion (Kainama et al., 2017). The Southern District Court of New York sentenced the defendants to 20 years in prison because they were legally proven to have engaged in massive-scale money laundering through Liberty Reserve.

Law enforcement against perpetrators is based on the United States Code (U.S.C.), the Anti-Money Laundering Act, the Intelligence Reform to Prevent Terrorism Act, and the Bank Secrecy Act (Cherniei et al., 2021). Confiscation of crypto assets as a tool used in money laundering requires a confiscation warrant to be issued to the service provider. All confiscated cryptocurrencies must be kept in "cold storage" on a secure offline device until transferred to a government-controlled custodial wallet. Authorities can cooperate with the Computer Crime and Intellectual Property Section (CCIP) if they experience difficulties accessing cryptocurrencies.

The United States has also implemented the "Travel Rule" to deal with money laundering through cryptocurrencies. Guidelines regarding the "Travel Rule" are described in Recommendation 16 of the FATF. Based on the "Travel Rules" in the United States, Virtual Asset Service Providers (VASPs) must promptly obtain, store, and transmit information about senders and recipients whose transactions exceed $3000. Under the "Travel Rules," Virtual Asset Service Providers (VASP) and financial institutions involved in virtual asset transfers (VAs) are required to collect and share the personal data of transaction senders and recipients. The United States took this step to prevent the rise of money laundering carried out through cryptocurrency. This provision will strictly supervise crypto asset owners.

Furthermore, for the first time, cryptocurrency was mentioned in United States law in November 2021. Provisions regarding cryptocurrency are contained in the Infrastructure Investment and Jobs Act. This provision refers to cryptocurrencies as digital assets. It is "any digital value recorded in the distributed ledger protected by cryptographic or similar technology as determined by the Secretary." Any organization or individual who "transfers digital assets on behalf of another person" will be considered an intermediary under the Infrastructure Investment and Jobs Act. For each violation, the centralized cryptocurrency exchange will issue a Form 1099-B (Blackstone & Turner, 2022). Of course, this is terrible news for the perpetrators of this crime because the number of assets and profits they own will be known and immediately given to the Internal Revenue Service. This results in the advantages of owned cryptocurrency assets that cannot be hidden.

Furthermore, the coin mixer is often used to make identification difficult. The United States has dealt with cases of coin mixer services being used to launder money through cryptocurrency. In August 2022, the U.S. Treasury's

Office of Foreign Assets Control sanctioned the Tornado Cash crypto mixer. Cryptomixer Tornado Cash, founded in 2019, has laundered around $7 billion worth of cryptocurrencies, including $445 million hacked by the Lazarus Organization, a well-known hacking organization in North Korea. The assets contained in Tornado Cash are then frozen, and every transaction to and from Tornado Cash is prohibited (Butts & Keller, 2022). The sanctions imposed are primarily aimed at money launderers.

B. Germany

Germany is a member of the European Union and a pioneer in forming inclusive regulations for handling Bitcoin, Ether, and other virtual currencies. Establishing a comprehensive regulation regarding cryptocurrency transactions was formed as a supporting rule for the existing anti-money laundering regulations. In conjunction with implementing the Fifth Anti-Money Laundering Directive (AMLD5), Germany, a member of the European Union, has adopted a new regulatory regime for crypto assets. AMLD5, a European Union regulation aimed at preventing the use of the financial system for money laundering or terrorism financing, applies to all EU nations. The existence of AMLD5 emphasizes the importance of virtual asset service providers adhering to AML obligations. The new money laundering law regime was passed by the German Parliament (*Bundesrat*) through "The Act on the Implementation of the Amendment Directive to the Fourth EU Money Laundering Directive" (*Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie*). The law came into effect on January 1, 2020, by amending the provisions of the German Banking Act (*Kreditwesengesetz* – KWG) and defining a new category of financial instruments, which includes cryptoassets (Herkströter et al., 2020).

Cryptocurrency in Germany is considered a personal asset, not a currency (Nubika, 2018). The German Federal Financial Supervisory Authority (BaFin), which is an independent public legal institution under the legal and technical supervision of the Federal Ministry of Finance, confirmed this. The BaFin classifies cryptocurrencies as units of account, which means cryptocurrencies are not legal tender. The German government stipulates that citizens or legal entities can buy or trade crypto assets. The trading is carried out through exchanges and custodians licensed by the BaFin. The exchange must meet the KYC and AML requirements.

A 2016 German Ministry of Finance study states that roughly 100 billion euros are "laundered" in Germany each year (Kinkartz, 2021). Germany experienced significant economic losses, which prompted the German government to make an effort to stop money laundering by enacting various regulations and tightening supervision in order to minimize money laundering.

The German Money Laundering Act (*Geldwäschegesetz, GWG*) regulates AML obligations. In particular, anti-money laundering obligations apply to trading platforms and crypto exchanges. By making crypto a new type of financial service explicitly regulated by the law, all of the general rules for money laundering can be applied to crypto assets. Furthermore, as a member of the FATF, Germany follows the recommendations of the "Travel Rule" guidelines. It establishes a maximum threshold of USD/EUR 1000 for cryptocurrency transactions. As a result, any cryptocurrency transaction involving more than USD/EUR 1000 may be suspected of being a means of money laundering. Virtual Asset Service Providers will then report to the BaFin information about senders and recipients on transactions that exceed these thresholds.

Furthermore, regarding the confiscation and follow-up of cryptocurrency assets that are strongly suspected of being the proceeds of crime, this will refer to the applicable provisions, namely the Criminal Code of Germany/*Strafgesetzbuch* (StGB), the German Criminal Procedure Code (*Strafprozessordnung*), the German Banking Act (*Kreditwesengesetz*), and the Money Laundering Act/ *Geldwäschegesetz* (GwG).

Paragraph 1 of Article 261 of the *StGB* states that criminally-related objects may be confiscated. These objects include those resulting from criminal acts, those used in criminal acts, those used to prepare for criminal acts, and those created to commit or prepare for criminal acts. The *StGB* also regulates in detail the confiscation of profits from criminal activity. This is explained in Paragraph 2 of Article 73 of the StGB, which states:

> "If the perpetrator or participant has benefited from the proceeds, the court also orders the confiscation of these benefits."

According to German law, prosecutors can seize cryptocurrency assets and profits. The intended profit is obtained when crypto assets increase in value due to price increases after being purchased. Thus, the Attorney General's Office can confiscate the value of the initial purchase plus the profits derived from these assets. The confiscation of cryptocurrency assets as a tool used in money laundering was carried out based on a confiscation order by the court. According to Section 111p, Paragraph 1, of the Strafprozessordnung, conducting an emergency sale of crypto assets is possible. This is due to the high volatility of crypto assets, which can lead to significant losses in value. Thus, crypto assets can be sold on an emergency basis to avoid a more significant loss of value. Prosecutors have the authority to order the sale even before the accused is convicted. After the verdict, those crypto assets must eventually be added to the state coffers (Finanzen, 2021).

C. Are Cryptocurrency and Money Laundering Regulations Adequate in Indonesia?

Cryptocurrency is the most popular money laundering tool perpetrators use to hide assets obtained illegitimately. This phenomenon is not only a national but also a global one. The Asabri Ltd money laundering case is clear evidence of this phenomenon, where the Attorney General's Office has difficulty confiscating cryptocurrency assets allegedly resulting from criminal acts of corruption. The BAPPEBTI regulates cryptocurrency as an investment commodity in Indonesia. The use of cryptocurrency assets as a tool used to commit money laundering is followed up based on the Money Laundering Law, the BAPPEBTI Regulation, and the CPC.

Based on the results of the elaboration explained in this study, there are similarities between Indonesia, the United States, and Germany. These three countries do not recognize cryptocurrency as legal tender. Furthermore, in the case of confiscation of crypto assets as a medium for a crime, Indonesia, the United States, and Germany will ask cryptocurrency service providers to send transaction reports to the authorized institutions accompanied by a confiscation order. The "Travel Rule" rules have also been regulated in these three countries, with different thresholds but the same goal. The "Travel Rule" can assist the investigation process by providing sufficient information so that the authorities can determine the source of the transfer of funds and the recipient. Transactions that exceed the threshold set by the "Travel Rule" will be suspected and investigated further.

There are differences in regulating cryptocurrency assets as a tool for money laundering between the United States, Germany, and Indonesia. The United States and Germany have included cryptocurrency in their legislation. The Infrastructure Investment and Jobs Acts of the United States have regulated cryptocurrencies. Furthermore, Germany has included cryptocurrency in the German Banking Act (*Kreditwesengesetz*) amendment through the Act on the Implementation of the Amendment Directive to the Fourth EU Money Laundering Directive. Meanwhile, cryptocurrency as a tool for money laundering has never been explicitly stated in Indonesian law. Cryptocurrency widely misused to facilitate criminal acts, presents an urgent need for Indonesia to regulate it precisely and comprehensively.

The United States has formed the NCET to stop money laundering through cryptocurrency as a form of law enforcement. NCET involves law enforcement focusing on cybercrime, cryptocurrency, and money laundering so that these crimes can be eradicated and followed up to the fullest. Then Germany has a specific agency to deal with this, namely the BaFin. The BaFin oversees active companies in Germany that provide services related to crypto assets and uncovers

and investigates related cases. Indonesia does not yet have a specific agency that regulates cryptocurrency as an asset that can be used to commit crimes. The BAPPEBTI only regulates crypto asset trading mechanisms, obligations of crypto asset traders, and other provisions regarding cryptocurrencies as investment commodities. Even though the regulation has implemented the "Travel Rule," it is not contained in it regarding law enforcement. Thus, these rules have yet to optimally accommodate the handling of these crimes. The Commodity Futures Trading Supervisory Agency does not directly investigate crimes committed through crypto assets.

Based on the comparison that has been presented, existing regulations in Indonesia are not yet ready to eradicate the use of cryptocurrency as a medium for money laundering. As previously explained, in Indonesia cryptocurrency does not yet have special regulations, even though cryptocurrency has the potential to be involved in cybercrimes and prohibited transactions, including money laundering. To be categorized as a cryptoready country capable of optimally handling money laundering through cryptocurrency, Indonesia still needs to develop further regulations regarding money laundering through cryptocurrency as a whole, including how transactions are carried out, prohibition of transactions through exchanges that have a high potential for money laundering, such as DEX , and a ban on transactions involving coin mixers. Developing this regulation was challenging for Indonesia because of the following things (FATF, 2014):

1. Cryptocurrencies have a high level of anonymity compared to traditional non-cash payment methods;
2. The global reach of cryptocurrencies increases the potential risk of AML and countering the financing of terrorism, making it difficult for law enforcement to monitor and enforce the law;
3. There is no centralized supervisory control, which complicates the investigation and seizure of suspected money laundering cryptocurrency assets.

However, developing comprehensive regulations regarding cryptocurrencies which means of money laundering is not impossible. A holistic approach and collaboration between government, regulators and financial institutions is needed to develop comprehensive regulations regarding this crime.

Furthermore, "passive detection" is a technique for identifying crypto-currency users through centralized services such as exchanges and virtual currencies (Rustem et al., 2019). Historically, network file access protocol data was transmitted unrestrictedly on local area networks (Widhiyanti et al., 2023). This protocol evolved into an encrypted form due to the increasing popularity of public cloud services on the internet and the importance of privacy in network

transactions (Berrueta et al., 2022). Consequently, today's traffic monitors cannot capture accurate information about disk access activity, and detection systems that rely on this must operate more efficiently. Several research studies show that no system can detect ransomware based on encrypted network file sharing activity. Reid and Harrigan (Reid & Harrigan, 2011) seek to contextualize blockchain using publicly available data. They effectively identify and use this data to map transactions between cryptocurrency addresses and monitor email addresses associated with specific wallets or addresses. Therefore, it is necessary to pay attention to passive detection methods to increase the readiness of Indonesian regulations in fighting cryptocurrencies as a medium for money laundering.

IV. Conclusion

In Indonesia, cryptocurrency as a money laundering tool has yet to be explicitly regulated in the specific act. The existence of the BAPPEBTI Regulation only regulates the mechanism of crypto assets as investment assets. The handling of cryptocurrencies used to facilitate money laundering refers to the Money Laundering Law, the BAPPEBTI Regulation, and the CPC. These legal rules are less relevant to existing developments because the "follow the money" principle is used in money laundering investigations. Details of all crypto transactions are distributed to all account holders, and analysis of transaction flows and values against the time the crime was committed should make it possible to find the pseudonyms of the crypto users involved and follow their transaction history. The challenge is connecting pseudonyms with real people; crypto's decentralized nature makes this difficult.

Furthermore, the United States and Germany have enforced legal rules regarding using cryptocurrency as a medium in money laundering optimally, starting with preventive efforts, the investigation process, and the imposition of law. This is supported by various regulations and legal arrangements that are already qualified. In order to prevent and eradicate the use of cryptocurrency as a tool for money laundering crimes, Indonesia can adopt the efforts made by the United States and Germany so that the handling of similar cases can be carried out effectively and optimally. First, Indonesia can form a law that specifically and comprehensively addresses cryptocurrencies. The law must accommodate the provisions of cryptocurrency not only as an investment asset but also as a money laundering tool and asset that may be misused to commit criminal acts. The law should include the confiscation of crypto assets, the development of passive detection methods to make asset tracking easier, prohibitions for owners of crypto assets to make their assets completely anonymous and obscure traces through coin mixers, private crypto purchases such as DEX, and indicators that suggest suspicious activity in crypto assets. The formed law will provide legal certainty to cryptocurrency assets as a means of money laundering. Then, the handling becomes more optimal and precise because there is already a comprehensive law, and there will be no differences in

perceptions between law enforcers in investigating these crimes. Indonesia also needs to form a specific agency that deals with money laundering crimes through cryptocurrencies. The agency must consist of law enforcement officials focused on money laundering and cryptocurrencies. This specific agency will later carry out various efforts to eradicate money laundering through cryptocurrency, from preventive efforts to investigating and pursuing crypto assets and perpetrators..

References:

Adiyatma, S. E., & Maharani, D. F. (2020). Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State. *Lex Scientia Law Review*, *4*(1), 70–82. https://doi.org/10.15294/lesrev.v4i1.38257

Amadeo, K. (2022). *What Is the U.S. Department of the Treasury?* The Balance. https://www.thebalancemoney.com/u-s-department-of-treasury-what-it-does-and-its-effect-3305998

Anika, I. E. (2019). *New Technology for Old Crimes? The role of cryptocurrencies in circumventing the global anti-money laundering regime and facilitating transnational crime* [University of British Columbia]. https://doi.org/10.14288/1.0379183

Baltrusaitis, J. (2023, June 8). *Massive crypto influx: 110 million new users enter markets despite regulatory fears*. Finbold. https://finbold.com/massive-crypto-influx-110-million-new-users-enter-markets-despite-regulatory-fears/

Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2022). Crypto-Ransomware Detection Using Machine Learning Models in File-Sharing Network Scenarios with Encrypted Traffic. *Expert Systems with Applications*, *209*, 118299. https://doi.org/10.1016/j.eswa.2022.118299

Biggs, J. (2019). *Polish Police Arrest Head of Payment Processor Tied to Bitfinex Crypto Exchange*. https://www.coindesk.com/markets/2019/10/25/polish-police-arrest-head-of-payment-processor-tied-to-bitfinex-crypto-exchange/

Blackstone, T., & Turner, G. (2022). Crypto Regulation in the U.S. – What's New in 2023? *Security.Org*. https://www.security.org/crypto/regulation/

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., Zhang, B. Z., & Cloud, K. (2019). *Global Cryptoasset Regulatory Landscape Study* (SSRN Scholarly Paper No. 3379219). https://papers.ssrn.com/abstract=3379219

Budhi, I. G. K. (2021). *Bitcoin (Potensi Tindak Kejahatan dan Pertanggungjawaban Pidana)*. Rajawali Pers.

Butts, D., & Keller, L. (2022). *What is The Future for Cryptocurrency Mixers After U.S. Sanctions on Tornado Cash?* Forkast. https://forkast.news/future-of-cryptocurrency-mixers-after-u-s-sanctions-tornado-cash/

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chainalysis Team. (2021, October 14). The 2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% With P2P Platforms Driving Cryptocurrency Usage in Emerging Markets. *Chainalysis*. https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

Chainalysis Team. (2022, January 26). DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate. *Chainalysis*. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

Cherniei, V., Cherniavskyi, S., Babanina, V., & Tykho, O. (2021). Criminal Liability for Cryptocurrency Transactions: Global Experience. *European Journal of Sustainable Development*, *10*(4), Article 4. https://doi.org/10.14207/ejsd.2021.v10n4p304

Coincub. (2022). *Q2 2022 Global Crypto Ranking: Germany goes head to head with the USA*. Coincub. https://coincub.com/ranking/the-coincub-q2-global-crypto-ranking-categories-2022/

Crypto Head. (2021). The 2021 Crypto Ready Index. *Crypto Head*. https://cryptohead.io/research/crypto-ready-index/

Departemen Komunikasi Bank Indonesia. (2022). *Peran CBDC dalam Memperkuat Pelaksanaan Mandat Bank Sentral*. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2417722.aspx

Department of Justice. (2022a). *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency*. https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

Department of Justice. (2022b, February 17). *Justice Department Announces First Director of National Cryptocurrency Enforcement Team*. https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team

Dewey, J., & Patel, S. (2023). *Blockchain & Cryptocurrency Laws and Regulations USA* (United Kingdom). GLI - Global Legal Insights - International Legal Business Solutions; Global Legal Group. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa

Enyi, J., & Le, N. (2017). *The Legal Nature of Cryptocurrencies in the US and the Applicable Rules* (SSRN Scholarly Paper No. 2995784). https://doi.org/10.2139/ssrn.2995784

FATF. (n.d.). *Asia/Pacific Group on Money Laundering (APG)*. Retrieved February 3, 2023, from https : // www.fatf-gafi.org /en /countries /global-network /asia-pacific-group-on-money-laundering--apg-.html

FATF. (2002). *FATF Annual Report 2001-2002*. FATF. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Fatfannualreport2001-2002.html

FATF. (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (pp. 1–15). FATF.

FATF. (2020). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

Finanzen. (2021). *Beschlagnahmte Kryptowährungen: Was passiert mit den digitalen Coins?*finanzen.net.https://www.finanzen.net/nachricht/devisen/bitcoin-co-beschlagnahmte-kryptowaehrungen-was-passiert-mit-den-digitalen-coins-10879638

Forgang, G. (2019). *Money Laundering Through Cryptocurrencies* [La Salle University]. https://digitalcommons.lasalle.edu/ecf_capstones/40

Ginting, Y. P. (2021). Pemberantasan Pencucian Uang dengan Pendekatan Follow the Money dan Follow the Suspect. *Mulawarman Law Review*, 105–114. https://doi.org/10.30872/mulrev.v6i2.442

Herkströter, C., Born, M., & Loeck, A. (2020). *Crypto Assets: Germany Introduces New Regulatory Regime*. Regulation Tomorrow. https://www.regulationtomorrow.com/de/crypto-assets-germany-introduces-new-regulatory-regime/

Husein, Y., & K, R. (2020). *Tipologi dan Perkembangan Tindak Pidana Pencucian Uang*. Rajawali Pers.

Internal Revenue Service. (2014). *Internal Revenue Bulletin: 2014-18*. Internal Revenue Service. https://www.irs.gov/pub/irs-drop/n-14-21.pdf

Kainama, M. M., Warno, N. D., & Setiyono, J. (2017). Pencegahan Dan Penindakan Penggunaan Virtual Currency Sebagai Sarana Kejahatan Pencucian Uang Melalui Dunia Maya (Studi Kasus Liberty Reserve). *Diponegoro Law Journal*, *6*(1), 1–13.

Kinkartz, S. (2021). *Terlalu Mudah Melakukan Pencucian Uang di Jerman*. https://www.dw.com/id/transparency-international-sebut-terlalu-mudah-melakukan-pencucian-uang-di-jerman/a-58196320

Kocegarovas, G. (2022, February 16). *Cryptocurrency money laundering risk: The best explanation of a 3-step process*. https://psplab.com/cryptocurrency-money-laundering-risk-a-3-step-process/

Krishnan, A. (2020). Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations. *Journal of Strategic Security*, *13*(1), 41–58.

Kusumaningtyas, R. F., & Derozari, R. G. (2019). Tinjauan Yuridis Kepastian Hukum Penggunaan Virtual Currency dalam Transaksi Elektronik (Ditinjau dari Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang). *Jurnal Penelitian Hukum De Jure*, *19*(3), 339–348. http://dx.doi.org/10.30641/dejure.2019.V19.339-348

Lemire, K. A. (2022). *Cryptocurrency and Anti-Money Laundering Enforcement*. Reuters. https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/

Lin, L. X. (2019). Deconstructing Decentralized Exchanges. *Stanford Journal of Blockchain Law & Policy*, *2*(1).

Mabunda, S. (2018). Cryptocurrency: The New Face of Cyber Money Laundering. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (IcABCD)*, 1–6. https://doi.org/10.1109/ICABCD.2018.8465467

Marzuki, P. M. (2013). *Penelitian Hukum (Edisi Revisi)*. Kencana Prenada Media Group.

Muttaqim, M., & Apriliani, D. (2019). Analysis of The Probability of Money Laundering Crimes toward the Development of Crypto-currency Regulations in Indonesia. *Indonesian Journal of Criminal Law Studies*, *4*(1), 29–40. https://doi.org/10.15294/ijcls.v4i1.18714

Nelson, J. (2022). *What Are Coin Mixers and How Do They Work? - Decrypt*. Decrypt. https://decrypt.co/resources/what-are-coin-mixers-tornado-cash-how-do-they-work

Nubika, I. (2018). *Bitcoin: Mengenal Cara Baru Berivestasi Generasi Milenial*. Genesis Learning.

Nurcholis, M. R., Suarda, I. G. W., & Prihatmini, S. (2021). Penegakan Hukum Tindak Pidana Pencucian Uang dalam Penyalahgunaan Investasi Aset Kripto. *JURNAL ANTI KORUPSI*, *3*(2), Article 2. https://doi.org/10.19184/jak.v3i2.26765

Pramudiya, K. F. (2021). Pertanggungjawaban Pelaku Money Laundering Melalui Binance Coin. *Jurnal Hukum dan Pembangunan Ekonomi*, *9*(1), 40–51. https://doi.org/10.20961/hpe.v9i1.52518

Rahma, A. (2021). Kejagung Mengaku Kesulitan Usut TPPU melalui Bitcoin di Kasus Asabri. *Tempo.Co*. https://nasional.tempo.co/read/1454815/kejagung-mengaku-kesulitan-usut-tppu-melalui-bitcoin-di-kasus-asabri

Rajagukguk, E. (2005). Rezim Anti Pencucian Uang dan Undang-Undang Tindak Pidana Pencucian Uang. *Makalah Disampaikan pada Lokakarya "Anti Money Laundering" Fakultas Hukum Universitas Sumatera Utara, Medan*, *15*.

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. https://doi.org/10.22225/jkh.2.1.2961.19-23

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, 1318–1326. https://doi.org/10.1109/PASSAT/SocialCom.2011.79

Ridwan, R. R. (2022). Transaksi Mata Uang Virtual (Cryptocurrancy) Sebagai Celah Terjadinya Tindak Pidana Pencucian Uang. *Jatiswara*, *37*(3), 352–362. https://doi.org/10.29303/jtsw.v37i3.415

Rohman, M. N. (2021). Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia. *Jurnal Supremasi*, *11*(2), 1–10. https://doi.org/10.35457/supremasi.v11i2.1284

Rustem, M., Sergey, K., Anastasia, K., Muhamat, G., Venera, G., & Aleksey, K. (2019). Problems of Criminal Responsibility for Illegal Circulation of Cryptocurrency. *2019 12th International Conference on Developments in ESystems Engineering (DeSE)*, 996–999. https://doi.org/10.1109/DeSE.2019.00185

Sajidin, S. (2021). Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran Di Indonesia. *Arena Hukum*, *14*(2), 245–267. https://doi.org/10.21776/ub.arenahukum.2021.01402.3

Sam, Y., Hutapea, M. R. M., & Setiawan, S. (2022). Legalitas Cryptocurrency dalam Tindak Pidana Kejahatan Pencucian Uang. *Jurnal Ilmu Hukum*, *18*(1), 108–120.

Soekanto, S. (2020). *Pengantar Penelitian Hukum*. UI Press.

Stobierski, T. (n.d.). *Decentralized Exchanges (DEXs) & KYC*. Persona. Retrieved February 20, 2023, from https://withpersona.com/blog/decentralized-exchanges-and-kyc

Utami, G., & Astuti, P. (2022). Analisis Yuridis Penggunaan Cryptocurrency (Bitcoin) Sebagai Sarana Tindak Pidana Pencucian Uang. *NOVUM : JURNAL HUKUM*, 144–158. https://doi.org/10.2674/novum.v0i0.50069

Ward, M. (2007). *Sydney bitcoin money laundering investigation: Six more charged*. Retrieved June 10, 2023, from https://www.smh.com.au/national/nsw/six-more-charged-in-bitcoin-money-laundering-investigation-20210311-p579ng.html

Wardhana, R. A. K., & Sularto, R. B. (2022). Studi Komparasi Formulasi Tindak Pidana Pencucian Uang di Indonesia dan Malaysia. *Jurnal Pembangunan Hukum Indonesia*, *4*(2), 227–244. https://doi.org/10.14710/jphi.v4i2.227-244

Widhiyanti, H. N., Hussein, S. M., & Ganindha, R. (2023). Indonesian Cryptocurrencies Legislative Readiness: Lessons from the United States. *Sriwijaya Law Review*, *7*(1), 150–172. http://dx.doi.org/10.28946/slrev.Vol7.Iss1.2138.pp150-172

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

Wijaya, F. N. A. (2019). Bitcoin Sebagai Digital Aset pada Transaksi Elektronik di Indonesia (Studi Pada PT Indodax Nasional Indonesia). *Jurnal Hukum Bisnis Bonum Commune*, *2*(2), 126–136. https://doi.org/10.30996/jhbbc.v2i2.2388

Wisnu, A. A. N., & Dharmawan, N. K. S. (2021). Legalitas Investasi Aset Kripto di Indonesia Sebagai Komoditas Digital dan Alat Pembayaran. *Jurnal Kertha Wicara*, *11*(1), 66–80. https://doi.org/10.24843/KW.2021.v11.i01.p07